The Human Firewall

by

Anirban Ghosh

A Thesis

Submitted to Examination Department

Indian Management School and Research Centre

In Partial Fulfillment of the Requirements

for the Degree Ph.D.

October 2021

APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED

Name of Student – Anirban Ghosh

Degree for which submitted - Ph.D. in Behavioural Security Management

Department – IMSR Examination Department

Thesis Title – The Human Firewall

Name(s) of Thesis Supervisor(s)

1.Dr. Avinash Singh

2. Dr. Pritam Malhotra

Month and year of thesis submission – October 2021.

Abstract

Hackers / fraudsters frequently use Phishing, Vishing, Smishing and social engineering attacks to gain an access into a target system or network. This type of attack is a marvelous challenge to protect, as the weakness mostly lies within us (humans), not in the technology. A robust security system contains more than just hardware or software; there must always be a “wetware” defense element as well. The “human firewall” is a concept in security awareness that enables a team to fight against hackers in a proactive as well as reactive fashion.

The first part of the research is targeted in creating a safer connected world by protecting our customers, ourselves, and the future from all possible form of Cybercrime to be one step closer to be the best-connected Company across the globe. By deploying a simple 18-month plan to build and deploy the Human Firewall, With the Sponsorship of Kevin Brown - Director of BT Security to start off with the feasibility check of the research with the team. Through this research currently we are deploying the brilliant Human Firewall for our internal customers and Our People. Through our internal workplace group, we did a trial with our brilliant community members who shared their opinion and some great feedback which helped us a lot. This research shows the importance and usefulness of Human awareness to build and deploy the strongest Human Firewall across BT. The benefit is not only limited to design and manage employee behavior but also it has a huge impact on the personal front of all the employees to spread awareness across all their loved ones, friends, and family members to stay safe from all these cyber-attacks.

The Human Firewall – Security is everyone’s responsibility

Copyright © 2022 Dr. Anirban Ghosh, Ph.D.

ISBN: 978-93-5627-641-3

Name of The Author – Dr. Anirban Ghosh, Ph.D.

First published in India in 2022 by the Author.

Please share with as many you can, because together we are the Human Firewall.

CERTIFICATE

It is certified that the work contained in the thesis titled “The Human Firewall” by “Anirban Ghosh” has been carried out under my/our supervision and that this work has not been submitted elsewhere for a degree.

Dr. Avinash Singh / Dr Pritam Malhotra

Signature of Supervisor(s)

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of BT Group plc.

To Sir, Bebo, Groot & Puntu

Acknowledgements

I would first like to thank BT Group plc specially to my mentor Michael Fortune for his invaluable assistance and insights leading to the writing of this paper. My sincere thanks also go to the members of BT Group for their patience and understanding during the two years of effort that went into the success of this research.

Additionally, I would like to thank My Mom and Mosai for the insights they gave and discussions we were able to have during the process of research; my Dad for his love and support; and my wife for her absolute and unconditional love and support through this very challenging task; she helped make it the most rewarding.

Most importantly, I would like to thank my Co-mentors Matthew Dalby, Dave Morris, Anita Duxbury, and Simon Newton for guiding me through this tumultuous last 2 years. Truly all things are possible through their help and support.

I would like to thank all my Friends and Family members for all their support, My High school teachers Monideep Sir, Manik Sir, Joydeb Sir for making me this able to come up with the idea of The Human Firewall.

Finally, I must thank my Mentor since my high school Captain Sujit Kumar Lahiri (41/1 Bengal BN National Cadet Corps) for making me realize and believe the abilities and power of a Human Being, Jai Hind Sir.

Anirban Ghosh

A message from my Mentor

“I have known and mentored Anirban in the human firewall and the key social engineering and insider threat risks for some years. Anirban has embrace the human firewall concept and has proven to be a great student in security behaviours and the risks from social engineering and insider threat.

He has developed his knowledge and learning with eagerness to become one of our key leads across India in this subject. He has a desire to learn and a passion to make a difference to protecting BT and our people.”

Mike Fortune

Security Behaviours Team Manager

BT Security - Protect BT Services & Operations

A message from my Co-Mentor - 1

“It has been a pleasure working with Anirban to deliver the Human Firewall initiative across our organization. He has a real passion for this subject which comes across when he is presenting the risks of social engineering to our business. He also keeps up to date on the key themes in the industry which enables his to keep refreshing the awareness program. What works well and drives positive engagement is that the awareness is not purely focused on how to protect the business, he also pays attention to how to protect your families away from work as well. This addition hook has proved to be a critical success factor as it shows that we are working to protect our employees in all scenarios and not just those that occur in the workplace. Anirban has proved to be invaluable to the team and as continues to look at new ways of keeping this topic fresh in the minds of our workforce.”

Matthew Dalby – CIPP/E, Int.Dip(GRC)

Director

Group Data Privacy, Compliance & Assurance

A message from my Co-Mentor - 2

“I’ve worked with Anirban to deliver Human Fire Wall training within BT and witnessed him explain the risks of social engineering inside and outside of BT to our colleagues in a personal and engaging way. His passion and knowledge for social engineering makes him an expert in this field within BT. The Human Fire Wall training sessions he has delivered add real value to people’s lives helping them protect themselves, BT, along with their friends and family too.”

Dave Morris - CIPP/E, Int.Dip(GRC)

Principal, GBS Risk and Compliance – Data, Security & H&S

Table of contents

List of figures

List of abbreviations

IT	Information Technology
GDPR	General Data Protection Regulation
IBM	International Business Machines
VP	Vice President
FTP	File Transfer Protocol
SMS	Short Message Service
PC	Personal Computer
CEO	Chief Executive Officer
OK	All Correct
EU	European Union
EEA	European Economic Area
EC	European Commission
ICO	Information Commissioner Office
VR	Virtual Reality
CSR	Corporate Social Responsibility
NGO	Non-Governmental Organization
COVID	Covid 19 Pandemic
ID	Identification
OTP	One Time Password
CPNI	Centre for the Protection of National Infrastructure

BT	Formerly British Telecom currently called BT Group PLC

I. Introduction

1.1 Overview

Organizations invest money in traditional IT protection so in a physical firewall, in antivirus, in email and web filtering, in sandbox technology and all those good things which are great but the biggest risk and also the greatest line of defense when it comes to cyber protection is actually the human firewall and the human firewall is the way that you and your colleagues and myself it's the way that we behave and it's the way that we respond to everything that's going on around us when it comes to any threat relating to technology.

As mentioned by Mike Fortune in the SE Podcast Security Awareness Series with Christopher Hadnagy on the Behavioural security “I think it's massive, I think we can't lose sight of the human condition you know and the part it plays in security. We can talk about technology and cyber all day long, but the reality is at the end of everything as a human being and we're very complex creatures, so it's got to play a major part in security and we often refer to it as the human firewall is what we call it. Getting people's human firewall switched on because it plays a crucial part in protecting the business and yourself”.

When I visualize any organization, I visualize it as a massive pipe as shown in Figure 1. That pipeline goes through the entire office building. It has got lots of rotations and turns and at every turn there's a joint and on the joint of that pipe is a member of your team. That member of the team must be responsible for their bit of the pipe. They have got to stop any of the leaks and it's not that long ago that when it came to cybersecurity it was put upon Information Technology team of the organization and it was thought of to be their responsibility. The problem is just way too big and it can no longer be the responsibility of Information Technology team of the organization and in fact legally since the introduction of GDPR in May of 2018 it's the responsibility of the directors of the business so it's no longer an IT problem you can't rely on one person your IT manager it's too big of a job for her to you've got to rely on all of your staff and your staff need to understand that they're the human firewall and they're your best line of attack so make sure you're educating to stay safe.

Figure 1:The Pipeline

1.2 Recognizing the Threat

While technical solutions like spam filters and mobile device management systems are important for protecting end-users, with the number of threats and the multitude of systems and communications through which staff performs work, the one unifying risk factor that must be addressed to improve fundamentally, security is the role of human error. Almost all successful cyber breaches share one variable in common: human error. Human error can manifest in a multitude of ways: from failing to install software security updates in time to having weak passwords and giving up sensitive information to phishing emails. Even as modern anti-malware and threat detection software has grown more sophisticated, cybercriminals know that the effectiveness of technical security measures only goes as far as humans properly utilize them.

If a cybercriminal manages to guess the password to an online company portal or uses social engineering to get an employee to make a payment to a bank account controlled by the cybercriminal, there is nothing that technical solutions can do to stop that intrusion.

IBM conducted a study into the cyber breaches that occurred among thousands of their customers in over 130 countries. This study was the most wide-reaching look into the causes of the cyber violations that had been performed at that point, but similar studies have since corroborated its results.

'Human error was a major contributing cause in 95% of all breaches.' — IBM Cyber Security Intelligence Index Report. One of the IBM study's key findings was that human error was a major contributing cause in 95% of all breaches. In other words, had human error not been a factor, the chances are that 19 out of 20 breaches analyzed in the study would not have happened at all.

Since human error plays such a vast role in cyber breaches, addressing it is key to reducing your business's chances of being successfully targeted. It also allows you to protect your business from a far wider range of threats than any single technical solution could - and can potentially empower your workforce to actively look out for and report new threats they may encounter. Mitigation of human error must be key to cyber business security in 2021.

1.3 The Cyber Psychology

Cyber Psychology is a relatively new discipline which really relates to the effects or the impact on us of technology in the way we think and behave and use technology. In simple term we can say that Cyberpsychology the study of the impact of emerging technology on human behavior. For example, we might use email or Facebook and we have sent a very attractive offer of say someone's inheritance which indeed sounds very attractive, but it might just be a scam. However, our emotional mind attaches itself to that beautiful offer, so we get lured into maybe responding to that email. If you take the example of the young people mainly teenagers using social media accounts, they get lured into emotional situations or relationships on social media quite often. If those relationships are going well then, their life is going well too. But if there's so some ruction or disruption of that emotional relationship that they form online then life isn't going to well and of course depending on who's involved in that relationship for example they can make the situation worse. So, there is a large element of awareness and training and support by the respective employers, local government groups, government and by parents and schools to help young working or school going people to let them know how to respond sensibly to their relationships and their communications and their reaction to interactions. I think probably having some basic understanding of what makes us think and what triggers are feeling triggers our behavior will help all of us. So, there's no real technology solution to this it's really a simple solution to spread as much awareness as possible from all possible side of our society.

In this context we must not forget about an emerging threat referred as “Internet Addiction”. According to Dr. Kimberly Young (1999) "Internet Addiction is described as an impulse control disorder, which does not involve use of an intoxicating drug and is very similar to pathological gambling". Some Internet users may develop an emotional attachment to on-line friends and activities they create on their computer screens. Internet users may enjoy aspects of the Internet that allow them to meet, socialize, and exchange ideas through the use of chat rooms, social networking websites, or “virtual communities.” Other Internet users spend endless hours researching topics of interest Online or “blogging”. Like other addictions, those suffering from Internet Addiction use the virtual fantasy world to connect with real people through the Internet, as a substitution for real-life human connection, which they are unable to achieve normally. The various types of Internet Addiction are: Information overload, Compulsion, Cybersex addiction, Cyber-relationship addiction and Addictions to video games and online role-playing games. Cyber world is the combination of computer and other communication convergence technology. A working definition is offered by Thomas and Loader (2000) who conceptualize cybercrime as those “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks” It is true that new multimedia technology presents uncontested opportunity worldwide to promote and progress human society. With this we must not forget that nothing is absolute in this universe and everything has its own merits and demerits. Same is applicable to the internet and new technology in the era of communication convergence. These internet and new technology can be used for commission of crime or to cause damage or injury to society.

As per Mary Aiken (2016) Human behavior has always been affected and shaped by technology, but there has been no greater influence, as far as I can see, than the advent of the Internet. You don't have to be an expert in the subject of online behavior to have observed that something about cyberspace provokes people to be more adventurous. The illusion is that the cyber environment is safer than real life -and connecting with other people online somehow carries fewer risks than face-to-face contact. But our instincts were trained and honed for the real world, and in the absence of real-world cues and other subtle pieces of information-facial expressions, body language, physical spaces-we aren't able to make fully informed decisions. And because we aren't face-to face when we are communicating and interacting with others online, we can be anonymous or more important, we feel we are As discussed in the prologue to this book, we can feel freed up and emboldened online. People can lose their inhibitions and in a way "act drunk" because, for some, being in the cyber environment can impair judgment and increase impulsivity. somewhat similar to the way alcohol can Disinhibition is facilitated by the environmental conditions of cyberspace-by the perceived lack of authority, the anonymity, as well as the sense of distance or physical remove.

1.4 The most common social engineering attacks

social engineering represents malicious online activities that trick people into revealing confidential information or providing access to resources usually money on a personal side and confidential or highly confidential including customer sensitive data on the organizational side. Cyber criminals have learned various ways of convincing people to transfer money provide information or download a file infected with malware. Five of the most common social engineering attacks are **- Phishing** which is one of the most common types of social engineering attacks where attackers use emails and text messages that contain links to malicious websites or attachments with malware. It's hard to ignore these cyber-attacks because they create a sense of urgency curiosity or fear among victims. In 2016 Verizon enterprise reported that 30 of phishing emails were opened by the recipient and 13 of those clicked on the link or attachment.

The second most common social engineering attack is **spear phishing.** Spear phishing targets specific individuals or enterprises these attacks are much harder to detect because the email is signed and looks like one a victim would normally receive from their it supports. For example, as a test beer phishing attack a security consultant pretended to be an i.t engineer he found out that 85 percent of employees whom he contacted gave out information which he had requested. In one of the biggest social engineering attacks carbonic attackers managed to record how the company's system works and steal almost one billion dollars.

The third most common social engineering attack is **baiting.** Cyber criminals use physical media such as flash drives with labels like payroll list or online forms to lure users into a trap. Those items seem beneficial but are loaded with malware.

The fourth most common social engineering attack is **scareware,** this type of social engineering attack often comes in the form of pop-up banners and alerts on the web browser. These makes the users think that their system is infected with malware and they must install the software that should help them. It is the malware itself.

The fifth most common social engineering attack is **pretexting,** the attacker usually pretends to be a co-worker company supplier police or bank official in that way attackers can easily get users to believe them and steal security numbers personal addresses and phone numbers or bank records from them.

1.5 Challenges to social engineering security

Social engineering incidents happen because of mistakes made by people. There are three top challenges of social engineering security the first is fear attackers use fear stress and anxiety that comes with filing taxes for example to send emails to victims stating they are under investigation for tax fraud.

The second challenge is curiosity, cyber criminals use events and news to take advantage of human curiosity. They trick people into opening emails by offering leaked data about a current trend or topic. For example, when Dr. A P J Abdul Kalam passed away a phishing message invited users to click a link and see an exclusive video of him saying his final goodbye.

The third challenge is helpfulness, an example of this is when an email is sent out to the staff requesting the accounting database password to ensure the manager pays everyone on time and employees take the bait and send it believing they are helping.

1.6 Technological advancement and cyber crime

As per The RAND Corporation There is no clearly articulated and globally accepted definition of cybercrime. However, many different definitions have been proposed by experts, industry, academia, law enforcement, governments, and international organisations. However, it is widely recognised that cybercrime crosses both the physical and the virtual worlds. The virtual aspect of cyberspace allows cybercriminals to disregard national borders and to target victims around the world at range and at scale, making it challenging to combat, investigate and prosecute. Nevertheless, most cybercrime has real-world implications despite its virtual context. Therefore, it is useful to distinguish between two broad categories of cybercrime:

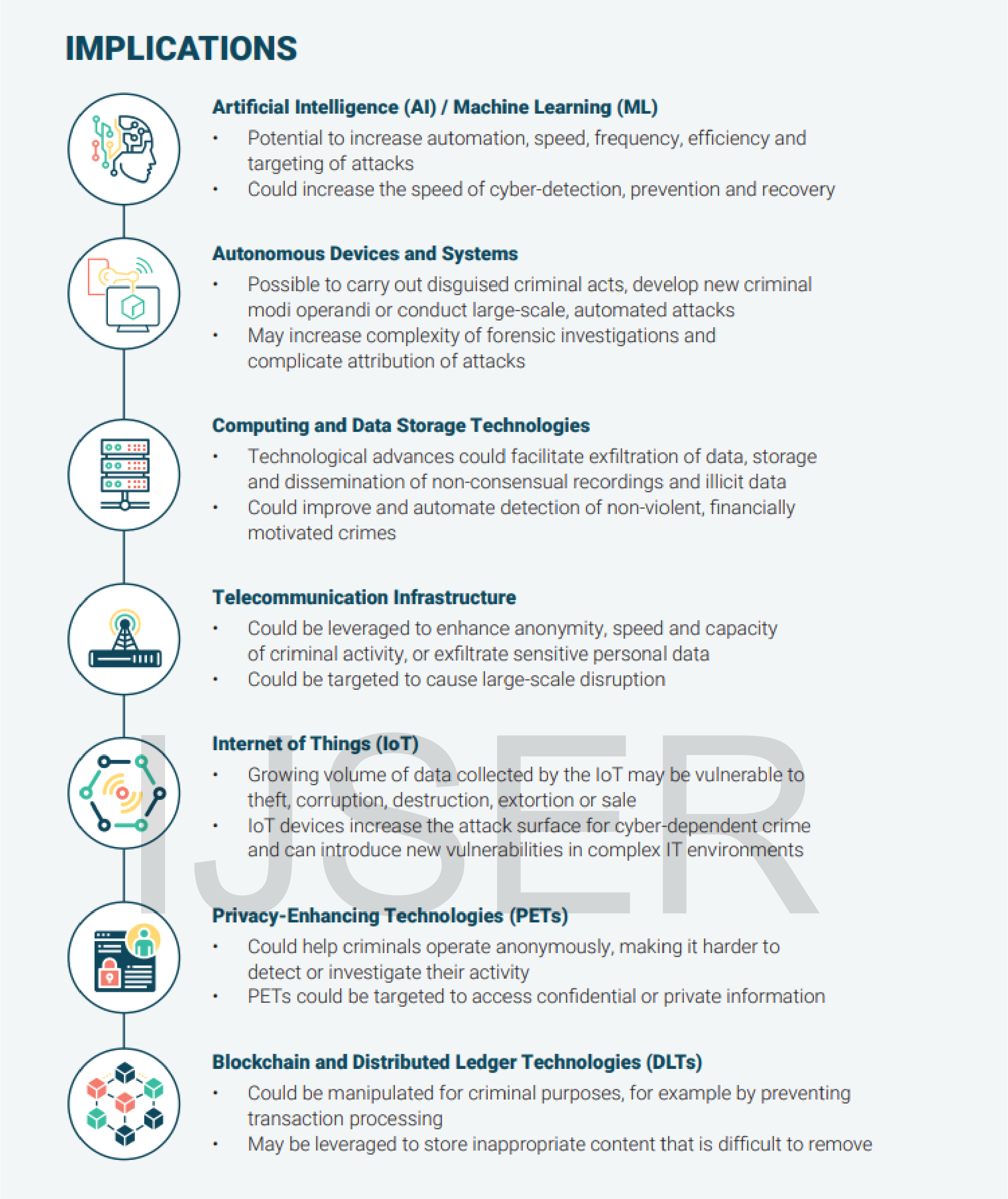
- Cyber-enabled crime refers to existing crimes that have been transformed in scale or form by the use of the internet, such as online fraud and forgery.

- Cyber-dependent crime refers to crimes that employ a digital system as the target as well as the means of the attack, such as the spreading of viruses or other malware and hacking.

This bipartite definition reflects the fact that certain forms of crime in the virtual world have their counterpart in the real world, as the internet's relative anonymity, ease of use, and transnational and borderless character are all features that create new opportunities for old crimes. At the same time, certain crimes are unprecedented in their ways and means compared to the pre-digital era. Digital systems and Information Communication Technology (ICT) are transforming society, services, and economic activity around the globe. But innovative new technologies can also create new opportunities for cyber-criminals to disrupt and defraud at scale. So how can governments and law enforcement agencies anticipate and tackle these emerging threats? RAND Europe's Centre for Futures and Foresight Studies (CFFS) employed horizon-scanning and serious gaming to identify potential trends and develop actionable insights. On behalf of the Estonian government, the European Commission asked us to assess how a range of new and emerging technologies might be used to commit cybercrime, and to propose ways to prevent or mitigate its impact. We identified seven emerging technology clusters (see opposite) with major implications for:

- Cyber-enabled crime – existing crime transformed in scale or form by technology, such as online fraud.
- Cyber-dependent crime – crime that employs and targets digital systems, such as hacking.

New and emerging technologies will not operate in silos, but rather build and interact with one another in ways that create broader opportunities and challenges. An array of cross-cutting trends and implications will need to be considered – for example, increased connectivity speed and coverage; the ability to collect and analyse more data; and increasing reliance on a few proprietary technologies as mentioned in Figure 2.



IMPLICATIONS

Artificial Intelligence (AI) / Machine Learning (ML)
- Potential to increase automation, speed, frequency, efficiency and targeting of attacks
- Could increase the speed of cyber-detection, prevention and recovery

Autonomous Devices and Systems
- Possible to carry out disguised criminal acts, develop new criminal modi operandi or conduct large-scale, automated attacks
- May increase complexity of forensic investigations and complicate attribution of attacks

Computing and Data Storage Technologies
- Technological advances could facilitate exfiltration of data, storage and dissemination of non-consensual recordings and illicit data
- Could improve and automate detection of non-violent, financially motivated crimes

Telecommunication Infrastructure
- Could be leveraged to enhance anonymity, speed and capacity of criminal activity, or exfiltrate sensitive personal data
- Could be targeted to cause large-scale disruption

Internet of Things (IoT)
- Growing volume of data collected by the IoT may be vulnerable to theft, corruption, destruction, extortion or sale
- IoT devices increase the attack surface for cyber-dependent crime and can introduce new vulnerabilities in complex IT environments

Privacy-Enhancing Technologies (PETs)
- Could help criminals operate anonymously, making it harder to detect or investigate their activity
- PETs could be targeted to access confidential or private information

Blockchain and Distributed Ledger Technologies (DLTs)
- Could be manipulated for criminal purposes, for example by preventing transaction processing
- May be leveraged to store inappropriate content that is difficult to remove

Figure 2: Implications of potential future cyber threats

1.7 Purpose Statement

The purpose of this paper is to introduce you with the product / solution called “The Human Firewall”. This product / Solution has a unique value proposition to help us nurturing a security-conscious workplace culture. We’ve identified that our behavior and the behavior of the people in our lives (at home and at work) is both the biggest threat and the best line of defense when it comes to cybersecurity. Together we are the Human Firewall. This human firewall has three main components: employee education, minimizing human error and getting ahead of new threats. But the main purpose of a human firewall is to raise the awareness of end users or employees to such an extent that they become a solid line of defense against attempts to compromise your systems or organization. Building a human firewall is more than just providing one-off security training, and it’s more than telling your users what’s bad and giving those boundaries. A human firewall seeks to stop humans from being the weak point in organizational security, by upgrading users to think securely. This product is capable to activate the firewall by the help of our social chatter and bring awareness and education to life which would not only transform the organization’s Security strategy but also impact the company’s brand image positively & equity across stakeholders globally. This prototype is not limited to any one Line of business or Domain, this solution may be deployed amongst all the employees across the organization irrespective of their geographic location. Everyone across the organization will be a part of the great Human Firewall.

1.8 Thesis Organization

This paper is organized as follows: Chapter two reviews a variation of related research that has been done on various social engineering attacks. Chapter three details the horizon scanning, and the research been done to identify the best possible solution to safeguard the employees from social engineering. Chapter four outlines how techniques designed to reduce an individual’s vulnerability to a social engineering attempt by switching on the Human Firewall. Chapter five discusses areas for follow up study as well as potential other areas of application for this research.

II. Literature Review

This chapter is a summary of the impressions connected with social engineering. First, the background of social engineering and how psychology previously has been researched in relation to social engineering is reviewed. Human Firewall models are then reviewed to give some background on how Human Firewall might be the showstopper to defend against any potential social engineering attacks. Finally, literature that deals specifically on how to develop a Human Firewall is reviewed for its potential applicability to defeat social engineering attacks.

2.1 Meaning of “Social Engineering”

One of the Mandatory behaviors of Human being are that we socially interact with each other. However, this is not an inherit skill this is a human skill that we learn as we grow up. In any way you can interact with another human being (e.g., in person, Over Phone, Over Chat/SMS, Over the social media platforms or Internet etc.) that's the social interaction.

Social Engineering is often referred to as a Phycological manipulation and influence people to give away information or do an act that can give away confidential or highly confidential data or information. Therefore, this is a well-known and one of the most popular tools amongst all the hackers and criminals. Often the word influence and manipulation get thrown around interchangeably. Let me explain how influence and manipulation compare and contrast. Influence is the process of getting someone else to what to do react think or believe the way you want them to whereas Manipulation is defined as exerting devious influence over a person for your own advantage. These definitions might sound very similar on the first look, but the difference becomes eminent as you pay more attention. Psychological manipulation is a type of social influence that aims to change the behavior or perception of others through indirect deceptive or underhanded tactics by advancing the interest of the manipulator often add another's expense such methods could be considered exploitative and devious this means that the person being manipulated is losing something while gaining nothing whereas the manipulator is gaining something and potentially losing nothing. Social influence on the other hand is not necessarily negative, the definition implies toward social political or economic power and power is neither good nor bad but how someone uses that power is what matters for example people such as friend's family and doctors try to persuade each other to change clearly and helpful habits and behaviors. Social influence is generally perceived to be harmless when it respects the right of the influencer to accept or reject it and is not unduly coercive but depending on the context and motivations it may constitute underhanded manipulation. Now if we look at the definition of social engineering as per Hadnagy (2018) "Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests." He also added while answering "Why is my definition so broad and general? It's because I believe that social engineering isn't always negative" and we can now relate back what he exactly meant by this statement. Unfortunately, the moment one use the term "Social Engineering" the only thought come into our mind is the negative side of it which is quite obvious as till date almost 85% to 90% of all multinational organizations have stated that they have been socially engineered in a negative way as depicted in Figure 2.

Figure 3: Social engineering attack

We may also say that Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data. When you hear the term "Social Engineering", this is the security industry's way of referring to a con or scan technique. It’s basically the art of gaining access to buildings, systems, or data by exploiting human psychology, rather than breaking in or using technical hacking techniques. Famous hacker Kevin Mitnick helped popularize the term 'social engineering' in the 1990s, although the idea and many of the techniques have been around if there have been scam artists.

Hadnagy (2018) remarks that When you understand how decisions are made, you can start to understand how a malicious attacker can use emotional triggers, psychological principles, and application of the art and science of social engineering to get you to “take an action that is not in your best interests” (p. 8).

2.2 History and Evolution of “Social Engineering”

While computer technology has only progressive enough to outgrowth the idea of security-based social engineering for the past few years, people have been using the moralities of human psychology to manipulate others for hundreds of years.

Doubtfully, the earliest accounts of social engineering-like strategic tricking trace back to the Trojan War in 1184 B.C. As per the story of the Trojan Horse trick, first mentioned in the famous novel The Odyssey. As the story goes the year was 1184 B.C. The Trojans and Greeks were immersed in a long, seemingly never-ending war. After a 10-year siege, the Greeks realized they had to get crafty to defeat the Trojans. They constructed a giant wooden horse and hid some of their army inside it as shown in Figure 3. The rest of the military sailed away, appearing defeated. The Trojans fell for the trick, dragging the wooden statue past their protective barriers as a trophy for their long-overdue victory.

After the sun went down and the Trojans went to bed, the Greek soldiers waiting inside of the horse snuck out and unlocked the gates around their city— sneaking in the rest of their armed forces who sailed back under the cover of darkness. The Greeks then used the element of surprise to destroy the city of Troy from the inside, formally ending the war. And therein lies the first recorded instance of social engineering.

Figure 4: The giant wooden horse as per Odyssey

Another example has been cited by Hadnagy (2018) which talks about one of the first documented stories I can find is in the Bible, in the book of Genesis, and it reportedly happened around 1800 BCE. Jacob wanted the blessing that was to be given to his older brother Esau. Knowing his father, Isaac, had failing eyesight and relied on other senses to know who he was speaking to, Jacob dressed in Esau’s clothing and prepared food like Esau would have prepared. Here’s the best part: Esau was known to be extraordinarily hairy, but Jacob wasn’t, so he fastened the skins of two young goats to his arms and the back of his neck. When Isaac reached out to touch Jacob, Isaac relied on his senses of smell, touch, and taste to tell him that he was with Esau rather than Jacob. According to the account in Genesis, Jacob’s social engineering attack worked. From the dawn of recorded history, we see one account after another of humans tricking, duping, conning, or scamming one another. On the surface, there might not be much that’s brand new when it comes to social engineering, but that doesn’t mean that nothing ever changes (p. 3-4).

While these acts of dishonesty were alive and well for nearly all civilized civilization, it wasn’t until ages later that someone put a name to this type of trickery— something more systematic and intentional than a simple trick. Calculated steps carefully scored to manipulate and break a barricade.

Hacker Kevin Mitnick helped to promote the impression of "social engineering" in the cybersecurity world in the 1990's, wherein bad actors engineer social situations to trick a person into taking an action.

Here's an example of how Kevin exploited users in the 90's:

In the 90's, Kevin Mitnick was once the most wanted cybercriminal in the country. In 1992, he became an escapee when he dishonored trial from previous cybercrimes by monitoring the voicemails of the authorities investigating him.

In hopes of being able to communicate confidentially and avoid arrest, Kevin set out on a pursuit to manipulate the technology inside the once high-tech MicroTAC Ultra Lite cell phone by Motorola. To fly under the radar and chat without being traced, Kevin decided to go after the source code in the firmware of the phone.

He began his social engineering siege by calling the directory to get the phone number for Motorola (a common practice before the popularity of Google). Kevin began small by asking to talk to the Project Manager of the MicroTAC Ultra Lite. A receptionist connected him to others, who transferred him many times until he finally got in touch with the VP for all of Motorola Mobility.

During Kevin's eight transfers prior to connecting with the VP, he learned a very interesting fact: Motorola has a research center in Arlington Heights. Under the pretense of an employee from the Arlington branch, Kevin asked again to connect with the Project Manager for the Ultra Lite. He socially engineered this Arlington branch pretext to gain trust and get an in with the VP— a key tactic these engineers use.

The VP gave Kevin the Project Manager Pam's extension, only to get a message that she was away on vacation. On her voicemail, she left a contact number to reach another person in her absence. Kevin called the contact, Aleesha, and asked if Pam left on vacation yet to create the illusion that he and Pam had connected prior, making his story all-the-more believable. He then told Aleesha that Pam promised him she'd send him the Ultra Lite source code but said that if she got caught up before leaving, Aleesha could send it.

He then instructed her on how to zip the files, since there were hundreds to package. But when he tried instructing her on how to transfer the zip to his anonymous FTP, the connection failed, and Pam asked him to hold while she went to grab her Security Manager to help.

It's here that Kevin panics, realizing that the jig could be up if security personnel got involved, suspecting foul play. But to his surprise, she returned with the security person's personal username and password to the proxy server to upload the file.

This clever narrative helped Kevin complete his mission and walk away with the source code. Although he didn't end up doing anything with the code, this type of highly sensitive property information could have easily been sold for high profit or been used as blackmail against Motorola for a generous payout.

While there's no arguing that the Trojan Horse story and Kevin's Motorola exploit denote powerful examples of manipulation, modern social engineering ploys involve more direct relationship building and clever storytelling over digital technology.

Bad actors attempt to compromise vast servers and networks of online data, with entirely new threat landscapes and vectors like email, Wi-Fi, routers, injected USBs, SMS, etc.

But because social engineering attacks are often conducted on complex, interconnected devices, it's harder to trace a breach than some instances from the '90s through the early 2000's.

Plus, even when an attack is launched, the breach is often stealthy, with the target sometimes having no idea they've been compromised for a length of time. In fact, the median length of time an adversary will sit inside a network undetected is an incredible 146 days. During these months, a hacker could dig deeper into a system, gradually uncovering more private data for financial gain.

Hadnagy (2018) mentioned about Dr. Paul Zak appeared in The Social-Engineer Podcast episode 44. He wrote the book The Moral Molecule (Dutton, 2012). In that book and in our podcast, Dr. Zak spoke about his research into a hormone called oxytocin. His research helped us to see how closely it is linked with trust because he made one very important comment about how oxytocin is released into our blood when we feel that someone trusts us. Please understand this very vital point: your brain releases oxytocin not just when you trust someone, but also when you feel that someone else has given you trust. According to Dr. Zak's research, this phenomenon has been demonstrated in person, over the phone, over the Internet, and even when you can't see the person who is doing the "trusting" (p. 8).

As per Hadnagy (2018) Another chemical that our brains produce is dopamine. Dopamine is a neurotransmitter produced by the brain and released during moments of pleasure, happiness, and stimulation. Blend oxytocin with dopamine, and you have a social engineering brain cocktail that can open any door you want. Dopamine and oxytocin are released in our brains during intimate moments, but they also can be released during normal conversations. Those conversations are at the core of social engineering. I believe we use these same principles daily—many times, unknowingly—with our spouses, bosses, fellow workers, clergy, therapists, service people, and everyone else we meet. Consequently, understanding social engineering and how to communicate with your fellow human is imperative for all people today (p. 9).

Oftentimes, it isn't until the bad actor takes the quest too far and is accidentally discovered through suspicious activity or boldly reveals themselves that the attack is even detected.

2.3 Email Scams – "Phishing"

t's a type of internet scam, a malicious email that tricks you into giving away information or downloading malware by clicking on a link or opening an attachment, typing in your user-id or password, replying or unsubscribing. Even, getting you to call a cybercriminal who is posing as someone you trust. Clicking on links in malicious emails could take you to fake websites (they can look very convincing) asking you to enter personal details like your password or banking details. If you open an attachment it can download malicious software onto our networks and systems, making them run slowly or even shutting them down. Stopping us from answering our customers calls or from attending their appointments. Or you could download ransomware allowing the scammers to freeze your computer and demand a ransom.

As per Hadnagy (2018) “The most talked about topic in the world of social engineering is phishing. In fact, the technical editor on this book, Michele, and I wrote about it in a book titled Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails (Wiley, 2016). (Yes, I did just shamelessly plug one of my other books.) Phishing has been used to shut down manufacturing plants, hack the DNC, breach the White House as well as dozens of major corporations, and steal countless millions of dollars in different scams. Phishing is by far the most dangerous of the four main vectors” (p. 10).

Figure 5: Phishing

There has been a recent resurgence of malware primarily spread through spam emails, a strain known as Emotet. This new tactic involves restarting old email conversations within a user’s Outlook email inbox and tricking the user into opening it by pretending to be someone they trust. The threat actors search for an old email chain in which the user has previously had a legitimate conversation with a colleague and then restarts that conversation adding in a malicious file. Malware is delivered via emails sent with malicious links embedded, or attached files, that when downloaded, enable to malware to propagate on the user's machine, and other machines in the same network. It enables threat actors to potentially gain control over a company's entire network, enabling data theft, loss of system control and potential failure of the IT infrastructure and restrictions on critical business processes. In extreme cases an entire company's network may have to rebuilt after infection!

2.4 Call Scams – "Vishing"

As per Hadnagy (2018) he mentioned "I honestly remember using the word vishing for the first time. People looked at me like I was speaking Klingon. Seriously, I might as well have said laH yIlo' ghogh HablI' HIv (you Trekkies will appreciate that). As of 2015, though, vishing was added to Oxford English Dictionary" (p. 3).

"Why is it important that vishing is now in the dictionary? It goes to show how much social engineering vectors have affected the world. Words that once appeared to be part of a "made up" language now are part of our everyday vocabulary" (p. 3).

"As I already mentioned, this is voice phishing. This has increased as a vector drastically since 2016. It is easy, cheap, and very profitable for the attacker. It is also nearly impossible to locate and then catch the attacker with spoofed numbers calling from outside the country" (p. 10).

Vishing is phone scamming. Criminals will use a phone call to try to persuade or frighten you into taking actions. They don't always make the calls in person often they're recorded – these are just as dangerous. Don't be tempted to select an option. Often, they'll use social engineering techniques by calling large organizations on numerous occasions to get tiny snippets of information as shown in Figure 5.

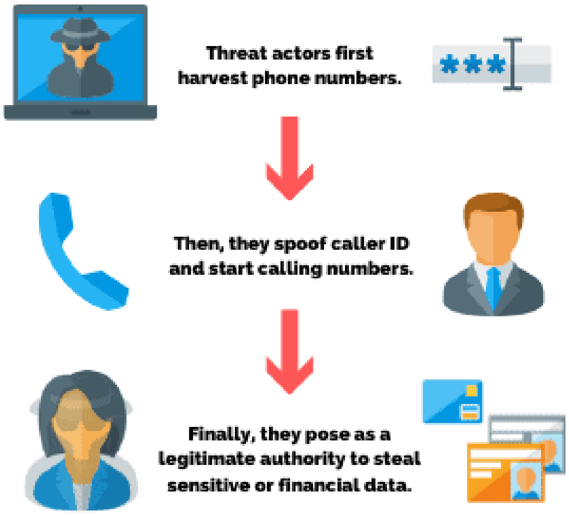

Threat actors first harvest phone numbers.
***
Then, they spoof caller ID and start calling numbers.
Finally, they pose as a legitimate authority to steal sensitive or financial data.

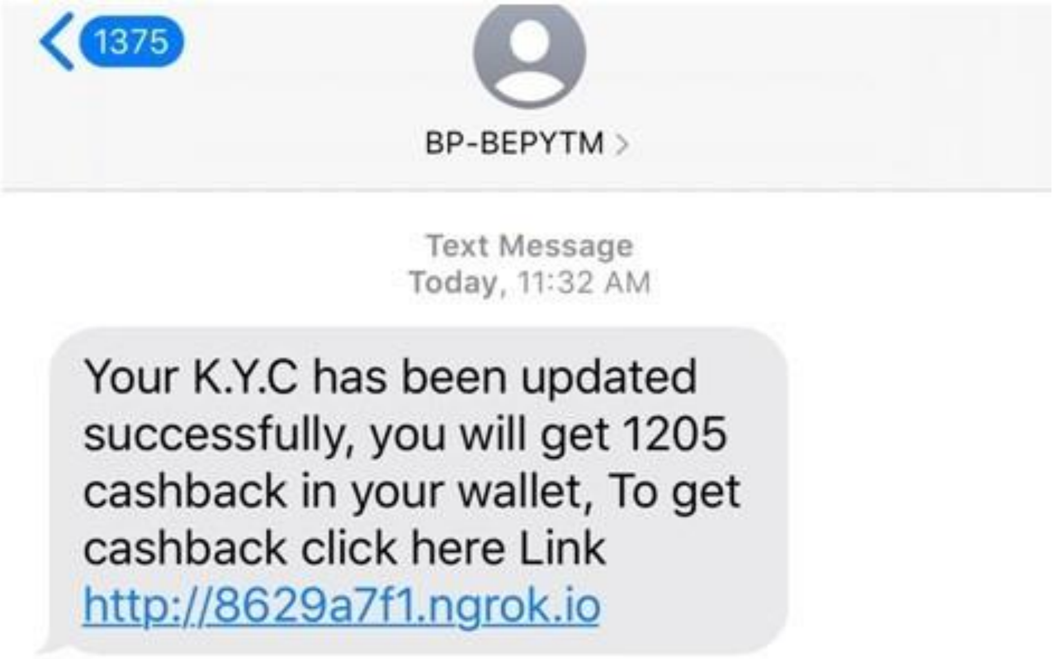
Figure 6: The Vishing process

Each piece forms part of a jigsaw which enables them to get their goal, information, or money! Social Engineers can be very convincing on the phone and they'll try to convince you to act. It could be to disclose customer information or persuade you to transfer money into their accounts. Even download malicious software so they can take control of your PC.

2.5 Text Scams – "Smishing"

Smishing is when cyber criminals send messages via text or on social media to trick you into disclosing information or downloading malware onto your device. As per Hadnagy (2018) "Smishing - Yes, this is a real thing, and it stands for SMS phishing, or phishing through text messages. With a simple click, these attacks were geared either to steal credentials or to load malware on the mobile device and sometimes both" (p. 9).

Once on your device malware can spread onto our systems and networks. As with phishing emails texts can include malicious links and attachments, or a good story to get you to do something to the scammers advantage. A sample of the most common smishing attack across India has shown in Figure 6.



Text Message
Today, 11:32 AM

Your K.Y.C has been updated successfully, you will get 1205 cashback in your wallet, To get cashback click here Link http://8629a7f1.ngrok.io

Figure 7: Sample Smishing attack

You could give away customer data and your own personal information such as your bank log in details and passwords. Even be tricked into transferring money to their accounts!

2.6 Spear Phishing

Spearfishing is a cyber-attack that uses personal information to target an individual the attack comes as an email, often disguise that someone you know or even a company into business with. These attackers do their research using the information you post it on social media such as where you work where you shop and bank and who you've connected. With this makes detecting this type of attempt much more difficult. For example, you may get an email that appears to come from a company you're familiar with containing a link for you to log into your accounts. You click on the link which takes you to a website that seems legitimate but it's a fake site designed to capture your login credentials.

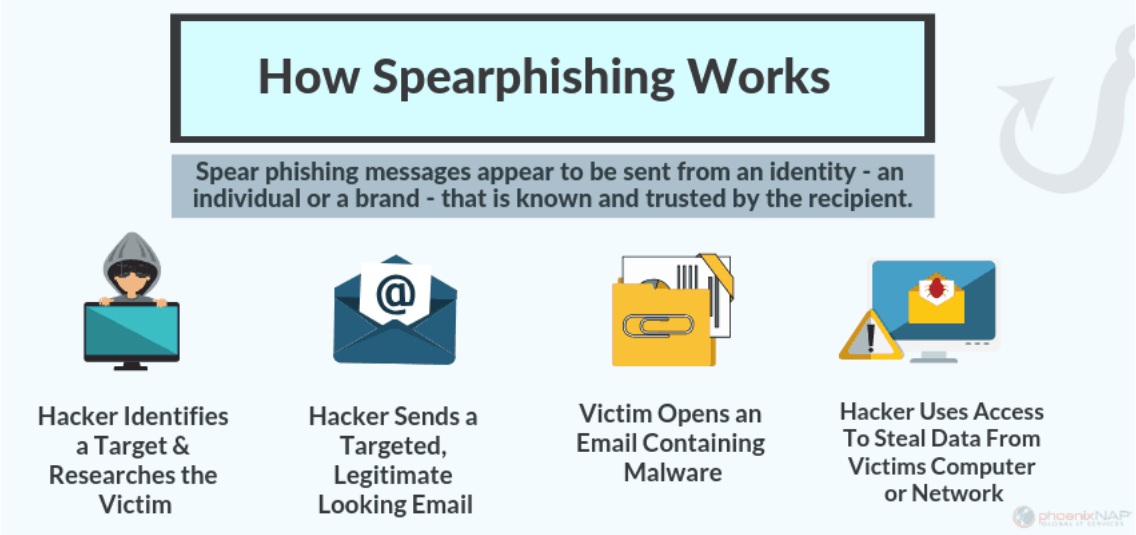

How Spearphishing Works
Spear phishing messages appear to be sent from an identity - an individual or a brand - that is known and trusted by the recipient.
Hacker Identifies a Target & Researches the Victim
Hacker Sends a Targeted, Legitimate Looking Email
Victim Opens an Email Containing Malware
Hacker Uses Access To Steal Data From Victims Computer or Network
phoenixNAP

Figure 8: The Spear phishing process

Once you enter your information it can then be used to make purchases as shown in Figure 7, bank withdrawals etc. or even sold on the black market. Just think about this how many of your online accounts have the same password and how many haven't been changed in years. The attackers will use this information to attempt to login to all major sites for their financial gain.

2.7 Whaling Attack

Like spear phishing, whaling is a highly targeted attack that goes after an organization’s “big phish.” Big phish are high-value individuals whose credentials or access to resources, if compromised, could endanger the entire business. In whaling attacks, big phish are carefully chosen because of their position within the organization. Whaling attacks also may differ from phishing attacks in terms of scope. The number of emails distributed is very small compared to a massive phishing campaign that might involve hundreds, thousands, tens of thousands, or more e-mails being sent. Whaling attacks can be more difficult to detect because they are stealthier and fewer in number. Attackers favor senior executives, high-level officials in private businesses, or even those with privileged access to government information. Often the content of whaling emails is high level, specifically designed for senior management, and can even take the form of an official report, containing highly confidential information. Sometimes emails can contain extremely personal content certain to appeal to the individual. Whalers also make proper use of corporate logos and leverage real, spoofed phone numbers. Because of the high-value targets, whalers can afford more time and effort into crafting the attack for far higher chances of success. A whaling attack is a method used by cyber criminals to masquerade as the CEO or a senior member of staff with the aim of stealing money or sensitive information.

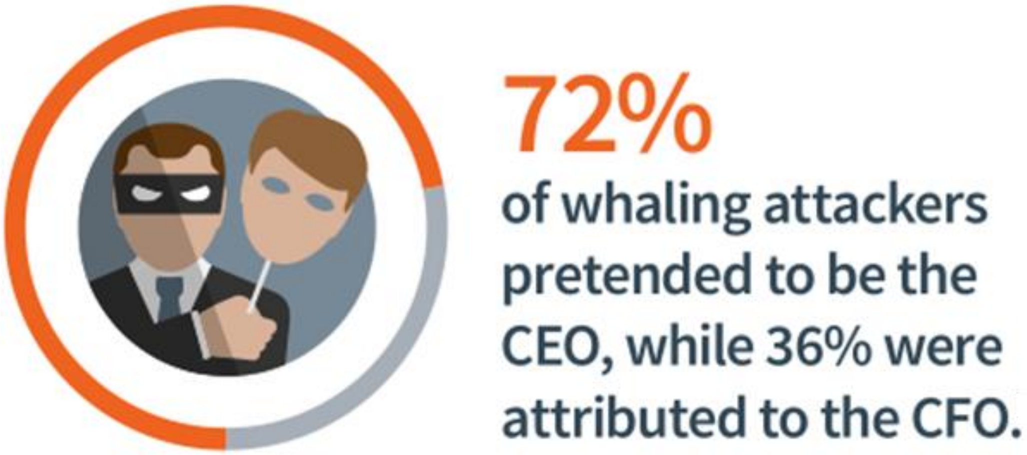

72%
of whaling attackers pretended to be the CEO, while 36% were attributed to the CFO.

Figure 9: The Whaling attack

Senior managers or CEOs of any organization being it large, medium, or Small in size doesn’t matter but all of them have access to Confidential company documents and the entire list of company employee and their data. Whaling attacks are usually done by sending a phishing email impersonating an employee who reports to the target, or the opposite way round. Some use underhanded tricks like sending a fake bill from a service provider connected with the organization.

III. Methodology

This chapter outlines the methodology used to properly compare social engineering attacks and Human phycological behavior. It provides the necessary information to deploy and switch on the Human Firewall for an effective Behavioural Security Management.

3.1 Problem Definition

This research talks about the specific areas which are the biggest concern of any organization regarding the potential social engineering attacks. This research determines whether social engineering can be connected to our behaviour and the behaviour of the people in our lives (at home and at work) and how to apply techniques shown to be effective against the problem of training someone to be resistant to any form of social engineering attacks.

3.2 Goals

The goal of this research is to explore more ideas to make a better solution to manage employee behaviour to protect the organization from any form of social engineering attacks. This research also focusses on the personal gaining side of the employees as they are not only vulnerable while working but these attacks may impact them in their day-to-day life or close friends or family members too.

3.3 Approach

A majority (70%) of consumers would stop doing business with a company if it experienced a data breach, according to a survey of more than 10,000 consumers worldwide conducted on behalf of Gemalto, the world leader in digital security. To find the exact challenges a survey conducted on random 2000 employees across the organization from 23 different countries and then the results are compared to identify the loophole in the current approach and propose a new and powerful approach. As per the survey conducted, we have identified that the current process is limited to share the outcome of any potential security incident only with the employee as shown in Figure 9.

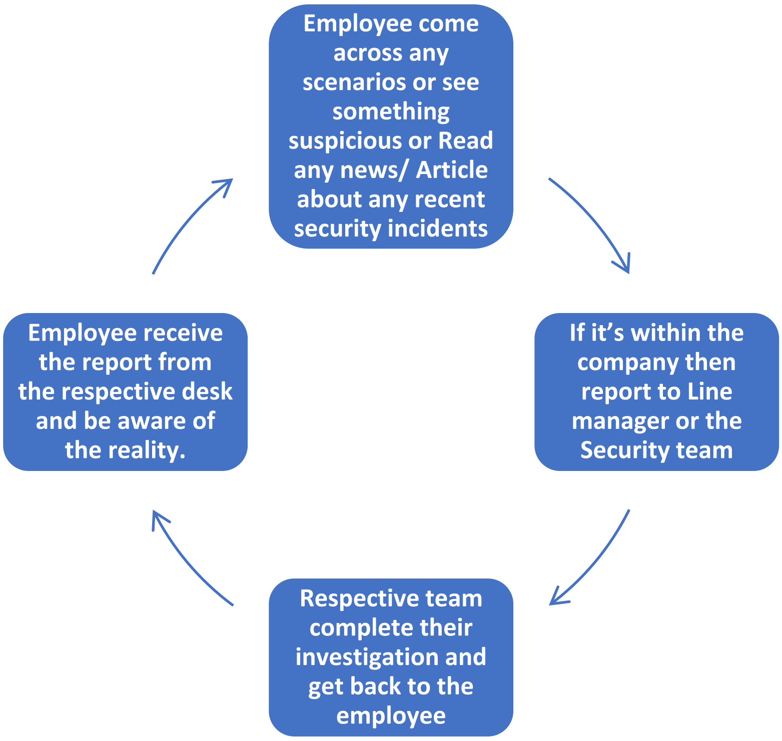

Employee come across any scenarios or see something suspicious or Read any news/ Article about any recent security incidents
If it’s within the company then report to Line manager or the Security team
Respective team complete their investigation and get back to the employee
Employee receive the report from the respective desk and be aware of the reality.

Figure 10: The existing Incident reporting process

This is the root cause behind the success of any future social engineering attacks done on the employees as we are not sharing any ongoing incident or awareness amongst other employees than the one who have reported the incident. So, this model needs to be updated.

After conducting another survey this time with a smaller group of people who are part of the organization’s security champions group approx. 200 employees their inputs been considered and a rough design of a new process been drafted, in Figure 10.

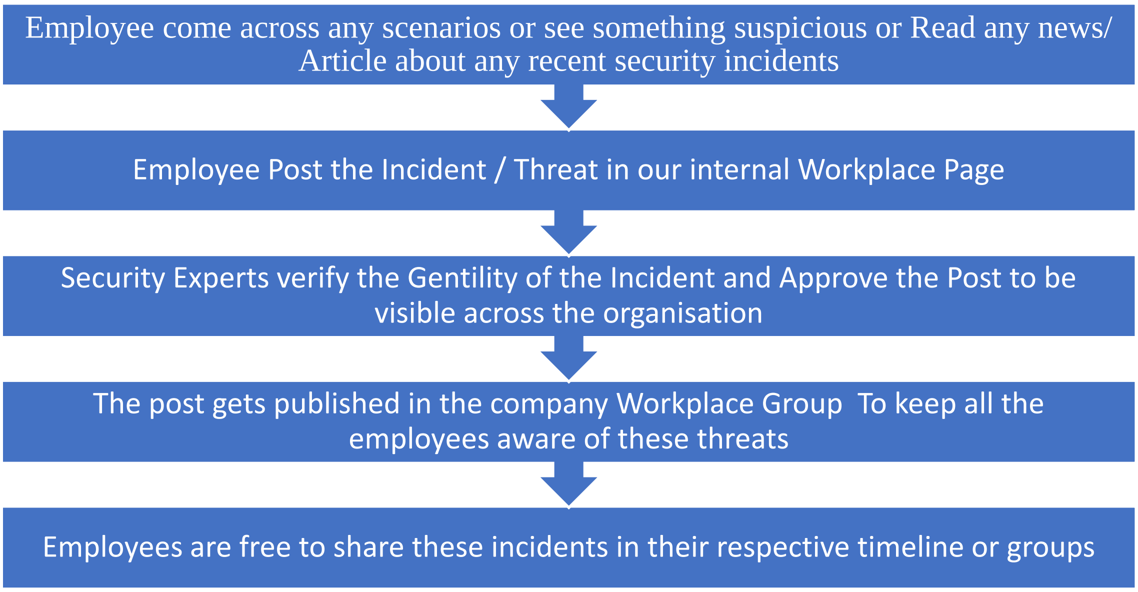

Employee come across any scenarios or see something suspicious or Read any news/ Article about any recent security incidents
Employee Post the Incident / Threat in our internal Workplace Page
Security Experts verify the Gentility of the Incident and Approve the Post to be visible across the organisation
The post gets published in the company Workplace Group To keep all the employees aware of these threats
Employees are free to share these incidents in their respective timeline or groups

Figure 11: The proposed Incident reporting process

On the survey the volunteers also provided their inputs regarding the future process. Out of all the suggestions provided by the security champions top 6 been picked to be considered while finalizing the results which may be linked in depth and in parallel in chapter four.

As per the surveyed Champions the following 6 elements must be prioritized to decide the results are as follows:

1. Make It Easy

It’s important to have long, detailed security policies that cover everything from password creation to mobile devices. But instead of overwhelming them, have your focus on strengthening a few weaknesses at a time.

2. Keep Education Ongoing

Many companies only have security awareness training once or twice a year, but this is clearly not enough. Cyber education should be continuous, receiving updates and briefs as new threats arise. Others should be educated whenever they change job titles as well as on a quarterly basis.

3. Give Incentives

Encouraging participation in any of the awareness initiatives can be as simple as giving each member special recognition for doing things like catching phishing emails. You can sweeten the pot with prizes or other awards. A recent study by the University of Oklahoma indicated that public attribution and validation were strong motivating factors in participation.

4. Include All Departments

People shouldn’t feel intimidated or that they aren’t tech-savvy enough to be a part of the solution. In fact, it’s essential they are encouraged to join. This particularly includes senior manager level employees who are often a target for spear phishing scams that steal identities.

5. Keep It Human

Those who wants must do their best to help others with cybersecurity concerns, thereby helping change culture and behaviour. Avoid treating people like cogs in a machine.

6. Always Be Evolving

The solution should be on constant alert for new threats, reporting any suspicious activity. As their tactics change, so must the team incorporate new best practices into their system.

3.4 Conclusion

During times of crisis, we tend to use our fast thinking, not our rational thinking. Rational thinking takes a bit longer to kick in, so when we feel under pressure, fast thinking may take over. But this can lead to us slapping our foreheads as we realize we decided too quickly; one that’s led to a mistake. And we’re facing pressure but from potential hackers who are trying to exploit the situation.

IV. Results and Analysis

The fact is, if you only focus on the digital part of security then you'll miss the most critical element: human behaviour. The easiest way to infiltrate any organization is through someone who works there. It's rarely malicious. People get distracted, make mistakes. It's human nature. Executives are optimistic about what technology can deliver in the workplace but what users do, or fail to do, can defeat the best-conceived security policies and solutions. Attacks don't need to be sophisticated. Phishing emails that include 'LinkedIn' in the subject line have an open rate of almost 50%.

There are big gaps between policy and practice. Employees don't admit to mistakes. Nearly half of employees say they personally have had a security incident and not declared it. Only one in three are 100% aware of the policies and procedures they should take to protect the security of their organization's data and less than half say they have received training on data security. There's a lack of confidence in training for new employees, and that steps are taken to protect data when people leave the company. What this suggests is that it's time to power up and reinforce the human firewall. Employees need to understand that they are a key line of defense in securing their organization. This requires (a) providing education and coaching in how to behave safely online, (b) helping employees appreciate the impact a breach would have on the organization and brand and (c) creating a culture in which it's OK to speak up, to admit mistakes.

4.1 The 3-stage thinking approach

Executives say their organizations are at more risk over the last year from (Refer to Figure 11):

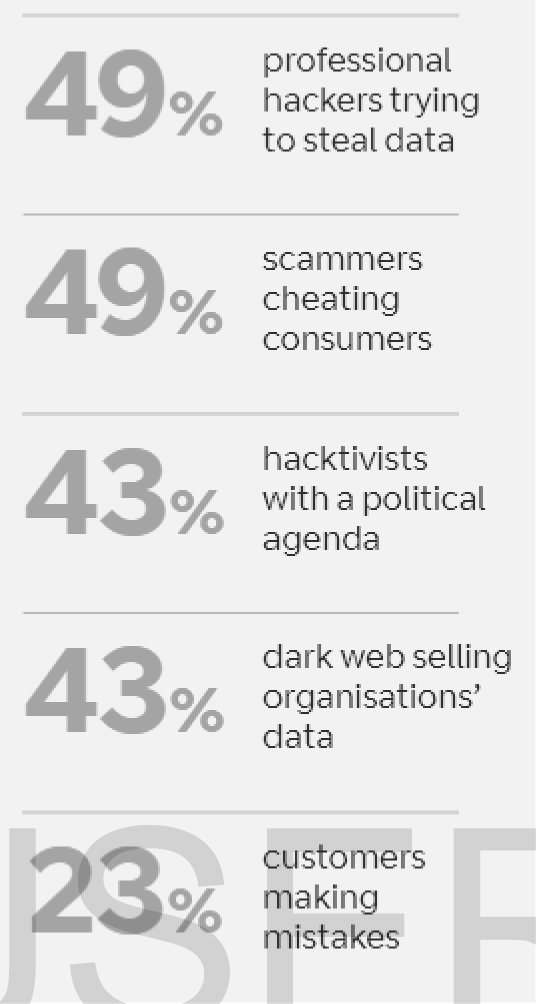


Figure 12: Organizational risk over F.Y. 2020 - 21

Human nature is part of the problem – and part of the solution. The fact remains that if you're only focused on technology, then you're missing the critical bit that is human behaviour. The easiest way to infiltrate any organization is through someone who works there. We need to super-charge the human firewall. In our organization, we adopt a 3-stage thinking process:

- ✓ **Stop -** If you receive a link or an attachment in an unfamiliar email, don't click it. Urgent subject lines such as "Your Account is Being Locked if You Don't…" or "Mail on Hold, Visit…" are signs that you could be reading a phishing email. We recommend you STOP for a moment and take a deep breath, These hackers or fraudsters always try to create a situation which demands urgency or immediate action this may be via Phishing / Vishing / Smishing. We must understand that when we are thinking too fast or reviewing such an urgent situation for the very first time it is our emotional brain who is taking the call and making the decisions and that's exactly what these hackers and fraudsters wants. So if we STOP for a moment and take a deep breath while dealing any of the situation which is urgent and which is asking to act upon something critical which may be personal or official then that will also us to switch over from our emotional brain to logical brain and then we can move in to Thinking.

- ✓ **Think –** Once you STOP and switch your thinking from emotional to logical brain, we must revisit the situation and ask some quick questions to ourselves. For example, if you have received an email which is either asking you for your personal information or asking you to click on a link then you must reread the email and ask yourself the below questions:

    - Do I know the sender? (Pro-tip: Look at the actual email address, not just the sender's name)
    - Is it asking for confidential information? (i.e., bank/credit card information or usernames)
    - Does something seem unusual or too good to be true? (i.e., You can click a link to win)
    - Is there an uncommon signature? (i.e., a company like Microsoft has a consistent signature line)

    Once you are done with all possible questions that may have come across your mind then you must move into the next stage which is PROTECT.

- ✓ **Protect -** Always protect your private information by asking yourself the above-mentioned questions. If you answered yes to any of them, complete to following actions to protect yourself and the business:

    - 1If you clicked on any links in the email, opened any attachments or replied to the email, immediately unplug your LAN cable or switch off Wi-Fi and call your company cyber security team to report or in case of the same is on any of your private device or with friends or family members then report to the respective local authority.

- Call the company to verify if they sent the email and report it if they didn't.
- Don't click links or attachments from an unknown sender. This will keep you from being sent to a malicious site.
- Report the email as junk mail and block the sender.
- Please stay alert and tell us about any other suspicious emails you receive in the future.

As we all face a new way of working, it's a process we think everyone could benefit from adopting. We're seeing hacking campaigns that are a mix of social media and emails. The subjects range from contacting you urgently about how to protect yourself from the Coronavirus, to how you've been identified as someone who's had contact with someone who's been tested as positive for the infection. These kinds of emails make you want to act. They make you feel that time is of the essence. They purposefully engage your sense of urgency, worry and fear.

Everything is moving so rapidly that normal procedures are impacted. Scammers are focused on this change in work mode. They're creating plausible stories (specialist cleaning companies) to draw you in, or making their emails appear to be from someone with financial accountability, or recommending a collaboration download that will make working from home easier. The more legitimate the email, the better the response.

They need just enough intelligence about an organization and who the accountable people are to be able to direct their emails. All they need is one or two people to act out of character (in good faith), and they could get the credentials of someone in the organization.

Or they'll try a broader scatter gun approach or a low, slow working of credentials in an organization - trying simple passwords that people may be using in haste, something users find easy to remember amongst the chaos – until they get access to a mailbox. Then they can set up a forwarding rule, so the user is completely unaware.

If you receive an email, no matter how legitimate, no matter how urgent, take a pause. Take a step back. Ask yourself, ‘Is what I’m being asked to do normal?’, ‘Is there anything strange about this email / instruction?’

If there’s a little niggle at the back of your head about it, pay attention. Think how you can verify if it’s real, how you can keep yourself safe, and who to report it to if you’re suspicious.

It takes no more than 30 seconds to engage your rational brain. Those seconds won’t make much of a difference to the right decision, but it could make all the difference in the world to the wrong one.

What this suggests is that it’s time to power up and reinforce the human firewall. Employees need to understand that they are a key line of defense in securing their organization.

4.2 Switch on the Human Firewall

The biggest advantage is that “The Human Firewall” can provide comprehensive human protection to your business. This will allow our employees to surf the internet as and when they need and ensure that they are already aware of all potential threats. It Allows Employees to Work Safely – With the best cyber security solutions for your business, you and your employees are constantly at risk from a potential cyber-attack. Human Firewall ensure everyone across the organization is strong enough to act as a firewall by blocking all possible loopholes to attack with the help of Education and awareness.

Moreover, Human Firewall Inspire Confidence in our Customers! If we can prove that our business is effectively protected against all kinds of cyber threats, we can inspire trust in our customers and clients. They will then feel more confident when purchasing our products or using of our services.

The definition of a human firewall is straightforward. It is essentially a commitment of a group of employees to follow best practices to prevent as well as report any data breaches or suspicious activity. The more employees you have committed to being a part of the firewall, the stronger it gets.

Our behaviour and the behaviour of people around us (at home and at work) is both the biggest threat and the best line of defense when it comes to security. Together we are the Human Firewall. Our human firewall has four main components: employee education, minimizing human error, getting ahead of new threats, and raising security awareness. Building a human firewall is more than just providing one-off security training, and it’s more than telling you what’s bad, it seeks to stop people from being the weak point in security, by giving you the tools and knowledge to think securely and stay safe by:

- ✓ Strengthening knowledge & awareness,
- ✓ Applying the right thinking and mindset in the key moments,
- ✓ Focusing and selecting the right actions and choices in the key moments,
- ✓ Embedding the right security behaviors and habits.

Security starts with you and security belongs to everyone and being security conscious means to helps to be engaged with, and take responsibility for, security issues. It indeed reduces overall risk of security incidents by increasing awareness of current threats and how best to deal with them. It also Increases reporting of security incidents allowing the organization to deal with issues in a faster and more effective way and to protect others. It helps fight against physical, reputational, or financial damage and helps to make a positive change in the small everyday decisions you make.

4.3 Never Trust Always Verify

“Trust is the glue of life. It’s the most essential ingredient in effective communication. It’s the foundational principle that holds all relationships” – Stephen R. Covey

I would like to echo the lines written by Elias Abouzeid in one of his blogs - Psychologically, we carry a powerful tool called trust. Trust increases our comfort level to allow us to speak and act more freely. But what if someone could develop an algorithm that could create trust, as human relationships do? Such an algorithm would make the human a part of the trust equation vulnerable. This kind of manipulation is known as social engineering, something that hackers rely on for 98 percent of attacks. In the FBI's 2018 Internet Crime Report, 26,379 people reported being a victim of a social engineering attack—costing nearly $50,000,000 in losses in just one year. A social engineer will manipulate their target using email, phone, or in-person tactics to acquire confidential information. Through observing personal mentalities, reoccurring routines, and relationships, the social engineer can develop the appearance of an individual you might naturally trust.

Across the industry security professionals are now shifting to a Zero Trust security state of mind. Regrettably one of the biggest problems we must address is to Trust Less and question more. In a country like mine, India where most of us grow up in a culture where since childhood, we always been taught to Trust people. Personally, I also believed and followed the same legacy for quite a few years. This is exactly what the cybercriminals or the fraudsters want you to do – to Trust. These fraudsters want you to trust their Phishing emails, Smishing text messages or Vishing calls. These attacks and scams are now a days all around us and this is the time when we must talk to our colleagues and educate our friends and families to trust less and question more. The biggest challenge is how we can get rid of this cultural obstacle, Well the solution is simple. With our research we have identified the most effective way to stop yourself been compromised by a fraudster is to follow and comply with our Stop -> Think -> Protect process. All what these hackers or fraudsters need is you to trust. These fraudsters may be considered as a highly talented artists who is a master in creating a situation where you will be forced to think by your emotional brain and that's it! The suggestion is that if you see an email that sets an alarm bell in your head then STOP for a few seconds and take some deep breath by doing that you shift your thinking process from emotional brain to logical one. Now you are good to THINK about the email or the matter and then you will start getting the actual inner guide and finally you will be able to POTECT yourself from these fraudsters or hackers as by then you must have already realized that with most things in life, if something appears to be too good to be true it usually is. So, it is important to STOP -> scams often distract our logical thinking and make us act on instinct or emotion instead. In these moments, stop and question your instincts. THINK -> ask yourself some basic questions – does it look, sound, and feel right? PROTECT -> what action can you take to protect yourself and our business? Can you challenge it, can you report it? This is how you will be able to switch on your Human Firewall. We will see more of this theme in the next Chapter through our CPNI campaign named “Think Before You Link”.

4.4 The Psychology of Social Engineering

On November 2003 President George W Bush visited Buckingham palace. The royal guard and the us agents believe they have taken every precaution to ensure their trip around so smoothly. Every branch of British security is involved to protect the president, every rooftop that might help a sniper is checked, they had told officers to look out for anyone acting suspiciously and inside the palace so there are armed guards. In the evening the queen the United States President George W Bush and prime minister Tony Blair will eat the dinner together. The security is at the highest level except for a minor detail! Two months before Ryan Perry a journalist from mirror was able to find a job as a foot man after applying to an advert on the official Buckingham palace website. He provided fake references on his cv and of course he didn't mention he was a journalist. During these two months no one checked his background, and he could walk freely around the palace taking pictures and serving food. Ryan commented that had I been a terrorist intent on assassinating the queen or President George Bush I could have done so with absolute ease. We have heard about stories of some of the most secure buildings and systems in the world are hacked by exploiting the weakest link in security which is the human factor. People tend to make mistakes; an employee might have a bad day. They might not be aware of the information they are giving or maybe they are tired of their job and just don't care anymore, so they might do something they wouldn't normally do.

V. Discussion

The last chapter focused on defining whether human behaviour or phycology could be associated to social engineering attacks. In this chapter we discuss and brainstorm to identify and implement the best possible methods that encourages a confrontation to social engineering. The priority while deciding these will remain the 6 suggestions provided by the security champions.

5.1 Workplace by Facebook

In our modern office culture almost, every organization are investing in creating their own internal workplace for collaboration amongst all the teams / people. This is a great platform to use to keep the Human Firewall switched on. In our organization we trial this using Workplace by Facebook.

Workplace by Facebook helps any organization to collaborate through group discussion, a personalized newsfeed and voice and video calls. The workplace account is separate from personal Facebook, let's look at each of the features that provided by this tool. For example, we can use groups for any of the project team of the organization. Whatever you like you have control over just how open or closed to make your groups. In a group make we can make a new post, we also can get a discussion started, we can add a photo, video, or document to get input from the rest of the team. We can respond to other posts and bring co-workers into the conversation too. Newsfeed gathers conversations from all the groups so that we never miss a project update. Company announcement newsfeed is tailored with important, trending, and relevant group conversations from across the organization. In workplace we can instantly follow any co-worker to get their updates and one’s newsfeed on their profile once can see who they are and how to get in touch including sending a message with work chat. We can follow a co-worker to stay up to date with their posts too. Work chat connects us instantly to any co-worker which is ideal for a quick one to one or you can loop in more people with work chat. It's easy to get everyone involved. We can use it to chat, share files, even make video calls with our team irrespective of their geographic location. Organizations use workplace to plan a company event and announce when and where it's happening and see exactly who's coming and get everyone talking before and after the event. It comes with a great search feature where you can just type the name or phrase you're looking for and get results from across the organization. We can also narrow our focus by searching directly inside a group or even a work chat conversation. Workplace helps us to stay connected to our organization wherever you are and will notify us when we have new messages or replies. We can get notifications by email on your computer or on your phone workplace too. Work chat also come as free apps for your Android or iPhone get updates even when you're on the move make your company more productive and connected with workplace by Facebook.

Figure 13: The Workplace by Facebook

With all these brilliant feature Workplace is the perfect platform to kick off with setting up a simple group and keep the same open to everyone to join across the organization. This will be used to share ‘Real –Time ‘warnings & alerts about Security Risks & Threats. We must adapt and responded well to the early feedback shared by our champions and this is the best possible solution based on the same. Success of the Human Firewall is predicated on 'volume take-up' and the proposed use of 'workplace' is a great example of leveraging technology to aid this. The approach being adopted is simplistic but relevant – it’s often the complexity that drives people away from good behaviour. Using Workplace and providing real examples of cyber matters will help provide a more detailed understating to our workforce. This is a great example of doing our best for our colleague - but with the added value that improving our internal estate will naturally help improve our service for our customers and arguably our Country.

How could this be improved - not only look at this for all the Employees but what if such an approach could be harnessed for all our customers and moderated in a way that helps improve all our organization’s cyber hygiene.

As mentioned above I have created an open group in collaboration with our entire Security team to help and support with any ongoing issues which all employees must be knowing to switch on their Human Firewall. In the early days as expected the engagement and participation across the organization were low however with more people getting involved and spreading the word, we have seen a massive engagement in recent days as shown in the Figure 13. We have also kept the option open to all the employees across the organization to post any potential fraud or security incident which may not be linked to the organization but could be imported to our personal life to be posted on the group. The post always goes through an Admin approval as a sanity check.

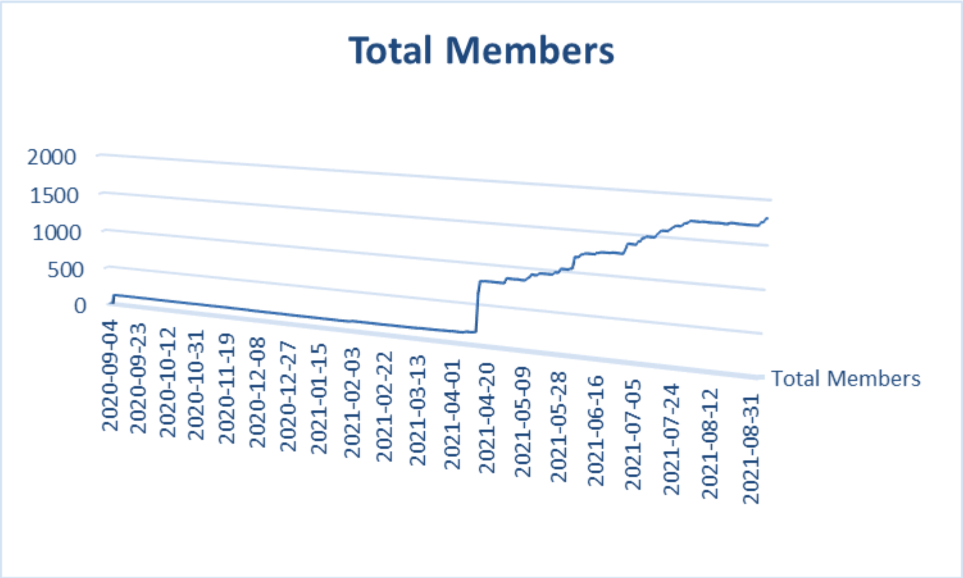


Figure 14: The engagement of members across the Company

5.2 One stop shop for all security needs

When you hear the phrase "one-stop-shop" what comes to mind? The words probably recall megastores where you can buy everything from food to clothing to household goods. However, stores like these are not the only businesses that can be "one-stop-shops". Any organization's security culture can be a role model to others if they have a simple solution in place like the megastores, where employees get all different variety of products and services offered by the organization to strengthen their security culture.

During the research it has been identified that more of all the organization have a robust security culture which include different security policies, incident reporting process, advise and guides, help for friends and families etc. all these resources are available to the employees via different internal portals / sites / SharePoint. In this situation if an employee is looking for some support may be related to a security policy to establish if an incident needs to be reported or not then the employee must visit the Policy page which normally sits within the Human Resource portal and then move to the security incident reporting page. At times it become too difficult for employees to keep a track of all these important pages and links of these.

What if a solution been created which may refer as a One stop shop for all security needs? This is exactly what been done within our organization. We did listen to all the feedback which made us in creating a one stop shop which is personal, Simple and Brilliant. Our employees can access all the security resources under one roof, and this has been a massive success to strengthen the Behavioural security of the organization.

This portal which referred as the One stop shop for all security needs can be referred as a brilliant tool which can be used as a part of organization's security behaviour and employee engagement and to keep the Human Firewall switched on. This portal may be divided into Five sub sections:

i. **Hot topics -**

If something is a "hot topic," then everybody is talking about it. If it's a "topic for discussion," then someone wants to have a serious conversation about it. Through this section we can talk about all kinds of latest and ongoing security concerns or topics with all employees.

ii. Advice & Guidance –

Through this section we will be providing all relevant Advices which will recommend a specific product or course of action for our employees to take given the circumstances and security goals and the Guidance is an impartial service which will help everyone to identify their options and narrow down their choices to strengthen employee's security knowledge.

iii. Training & Engagement

In this section of the page provides information on all available trainings and engagement resources of the organization related to security. This section helps employees not only to view and register for any upcoming live training sessions but also provide all the recordings of past trainings along with all different opportunities to get engaged in security related activities across the organization.

iv. Security & You

This section is dedicated as the Security Champions network which provide details of what, how, and why to be a part of it. it's always great when it's an optional program of many organizations including us when they start to turn the corner and say it's required, or we must, or we shall have a security champions network in place. The fun starts to dissipate and when people are showing up to the trainings and it's because someone told them. It's not going to be great as opposed to that security champion that's opted in for that buffer of a certain percent of their time to say they here because they heard that they get to learn how to break things. This section helps in providing this visibility and platform to all potential security champions across the organization.

v. Communications

The purpose of this section is to help everyone in the business to understand what we're doing and where we're going in the security space. This directly helps to create a community of advocates working for one company with a shared vision and purpose. With so much going on, internal communications have never been more important. The team will deliver communications that will encourage and support everyone across the organization, so that everyone can play their part in making the company a brilliant place to work. It's challenging, at times exhausting, but it's also hugely rewarding and fun.

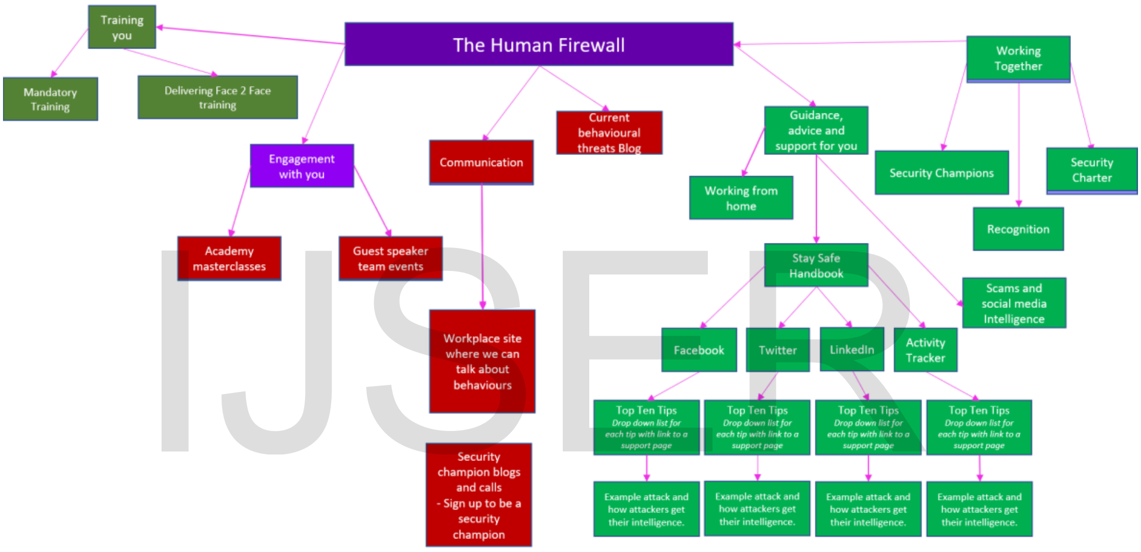

Training you
Mandatory Training
Delivering Face 2 Face training
The Human Firewall
Engagement with you
Academy masterclasses
Guest speaker team events
Communication
Current behavioural threats Blog
Workplace site where we can talk about behaviours
Security champion blogs and calls - Sign up to be a security champion
Guidance, advice and support for you
Working from home
Stay Safe Handbook
Facebook
Twitter
LinkedIn
Activity Tracker
Scams and social media Intelligence
Working Together
Security Champions
Security Charter
Recognition
Top Ten Tips
Drop down list for each tip with link to a support page
Top Ten Tips
Drop down list for each tip with link to a support page
Top Ten Tips
Drop down list for each tip with link to a support page
Top Ten Tips
Drop down list for each tip with link to a support page
Example attack and how attackers get their intelligence.
Example attack and how attackers get their intelligence.
Example attack and how attackers get their intelligence.
Example attack and how attackers get their intelligence.

Figure 15: The one stop solution portal structure

5.3 Considering the personal side

The General Data Protection Regulation is a regulation in European Union law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. If we investigate the GDPR Article 32(4) is concerned with the activities of employees and other workers who act under the authority of the controller or processor. The thrust of the requirements within Article 32(4) has traditionally been regarded as confidentiality issues in European data protection law (see Article 16 of

Directive 95/46/EC), but whilst Article 32 itself does not make this distinction, when it is read in conjunction with Article 5(1)(f), which is summarized as 'integrity and confidentiality, and Article 28(3) (b), which says that persons working under processors must work under a duty of confidentiality, it is highly likely that, in practice, the logical reasoning that has applied to date will continue to apply to the GDPR.

As such, it seems that all people who have access to personal data through their work for controllers and processors are working under circumstances that are tantamount to creating a duty of confidence. The essence of Article 32(4) is that these people must act within the boundaries of their instructions. They should not subvert the controller's position.

So, for example, they must not misuse personal data to their own advantage or to another's advantage, as would occur through unauthorized disclosure to third parties or by the making of unauthorized copies.

In security terms, the risks posed by employees and other workers is often referred to as 'the insider threat: Controllers and processors alike should have robust policies that alert employees to their responsibilities in handling personal data, provide them with role-based and regular training, and make clear the consequences for violating policy dictates. Employees may be subjected to reasonable forms of monitoring, but their employers should be careful not to stray into commenting workplace privacy violations.

You Can Have Security Without Privacy…
…But You Cannot Have Privacy without Security!

Figure 16: The quote on Security by ICO

If we talk about personal cyber security of all the employees, then it is important for any organization to ensure to educate and spread awareness around all the major steps that to protect employees and their families' data from hackers and malware. This is how an employee of the organization become more responsible and switched on not only while working but also in day-to-day life. we're helping to support kids, older and vulnerable people through free support, which will help them to get online and make the most of the digital tools modern life increasingly depends on. Out of thousands of such trainings and courses. For a quick overview I would like to call out Five top trainings and courses which not only available to the friends and family members of our employees, but these are available for anyone and everyone across the globe:

i. **Supporting your kids online with Rio Ferdinand –** In this episode, football legend Rio Ferdinand shares some insider tips for helping your kids use the internet safely.

ii. **Image vs reality: a families' guide to online influencers –** Online influencers are a big part of the online world, and hugely popular with our children. In this interactive video, we delve into the role of influencers, Image vs reality, the reality of being one, and lots of useful tips and topics which you can discuss with your child.

iii. **ONLINE SAFETY - Gaming consoles and platforms –** Set the right level of protection on gaming devices to give children a fun and safe experience with these how-to guides. This includes Step-by-step instructions to set controls on popular gaming consoles and devices, how device controls work, and get access to a list of resources and articles for further advice.

iv. **Parent controls - entertainment and search engines –** In this training one will learn to follow simple steps to set controls on sites and apps to make sure your child doesn't stumble across things they shouldn't. This also talks about Step-by-step instructions to set controls on popular entertainment services & search engines and get access to a list of resources and articles for further advice.

v. **Parental controls - broadband and mobile networks –** This training contains See step-by-step guides on how to manually set filters to limit the inappropriate content a child might see online with step-by-step instructions to set controls on major broadband providers and mobile networks, the limitation of network filters and get access to a list of resources and articles for further advice.

5.4 Technological advancement of trainings

To addresses a dilemma that most employers including us are facing is that all employees need to upgrade their security skills, learn new ones, or complete security and compliance mandatory trainings, but in-person or online training may not be an option in the current generation or environment specially when we are talking about a multi-national organization with huge employee base covering most around 20+ countries across the globe. Yet, training is especially important now, as employees strive to learn skills, and it may become even more critical with the advancement of threats and social engineering attacks changing and upgrading their pattern and approach on a regular basis or quite frequently. How can employers deal with this challenge?

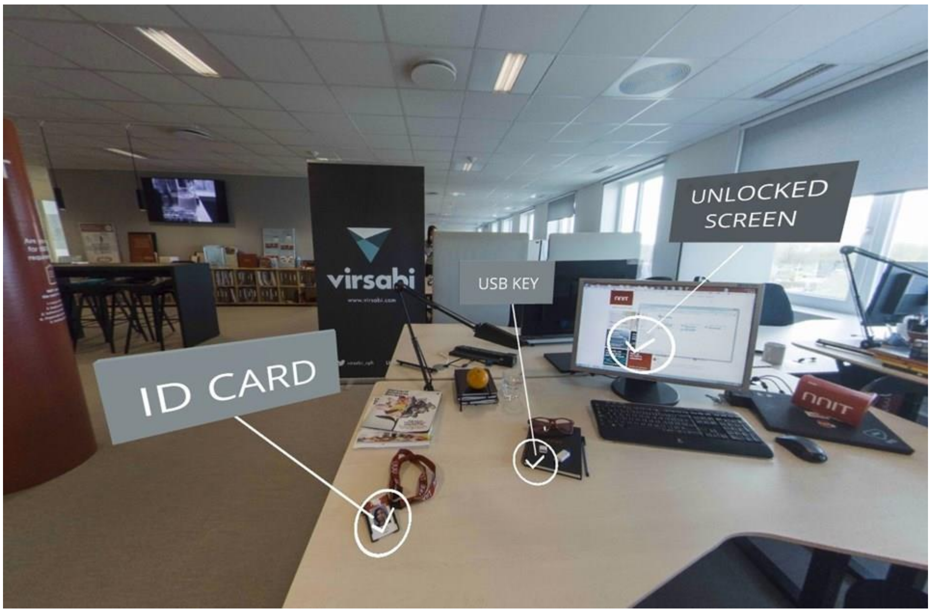


Figure 17: Sample Virtual Reality Security training

One solution to this training problem comes from an unexpected place: virtual reality as shown in the figure 16. Virtual Reality is already known to be effective for teaching hard skills and job skills simulations, such as pilots using VR-based flight simulations. But many employees also need to learn security skills, such as identifying a risk / threat and report or mitigate the risk. It's been shown that learners using VR become four times more engaged than when using traditional training methods. It also improved retention and confidence by 275% are four times faster to train and can reduce site costs and site-related safety risks as shown in the figure 18.

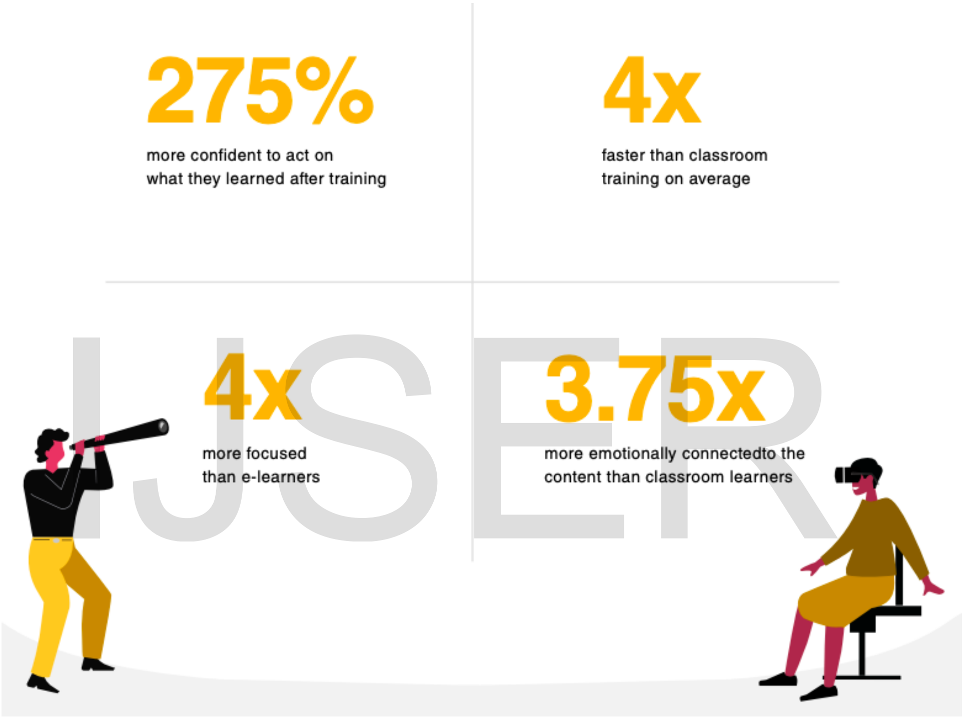


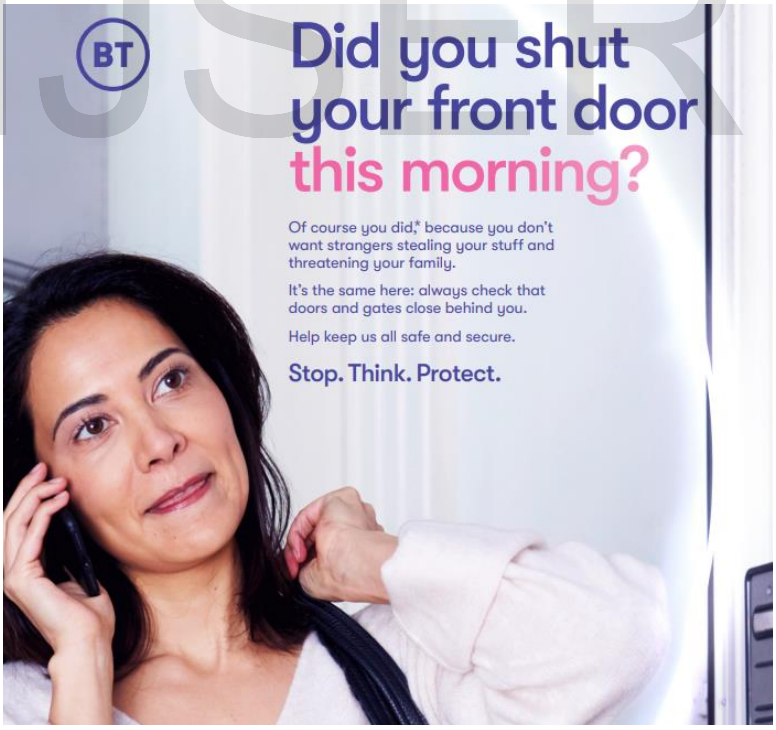
Figure 18: The impact of Virtual Reality Training

On the other hand, it’s also true that not everything is suitable for VR, that's why we suggest a blended learning approach using 3d animated e-learning packages for theoretical information and VR training for practical components. Why use slideshows and pdf documents to train the employees when organization could be providing them with immersive engaging and safe virtual environments to practice security procedures and experience sites without having to travel using a portable and easy to set up Virtual Reality headset. Virtual Reality is the most immersive learning technology on the market. It is unparalleled in giving employees a powerful sense of presence in the virtual environment, this technology has been rapidly adopted and heavily invested in by a wide variety of industries for training in both security and compliance. A big question which any of the organization may have is, they want to do virtual reality but what's it going to cost? And the most common response will be that it depends. I'll say the same thing that it does depend but to give some numbers to work with, an organization could do a virtual reality pilot for as little as $20,000, they could also do a full VR program for $150,000 or more. There are a lot of factors to consider, what are we training on? What's our starting point of training? Are we getting onsite and filming? Are we completely recreating something computer-generated? So, there are a lot of factors that come into play to determining the cost, but the entry point has gotten considerably lower. I think for organization who may have been considering an e-learning or a video may dip their toe in the water with VR because it's not $100,000 to do a VR program anymore. It's just not, it can be, but the price point has come down dramatically. So, it's a wide range but it's been seen that organizations can get things done for $20,000 and they can also spend well into the six figures.

5.5 Make it “Personal”

Let’s begin with our Behavioural Security Subject Matter Expert Mike Fortune’s statement “When it comes to security, it’s people’s positive behaviour that makes all the difference. Security must be a personal thing. You wouldn’t let complete strangers walk around your home. It’s the same with your office. It’s brilliant security behaviour that keeps us all protected. But security can be seen as a big stick that only strikes when we’ve done something wrong. That’s why we want to recognize the huge benefit of what we’re already doing right.”

In our education for BT as we try to make things personal and real that's what we want to do. Because we want to focus on the human side and we use that to really drive education to get people interested, aware and focused on the cyber and physical security, because at the end of the day it's about our behavior more than anything else. In our communication we utilize social engineering to make the education, the engagement very powerful. We got a great belief that the more people are aware the better choices they can make and so we've got this mission to really switch people on a bit more about being aware about being human being what it means to our behaviors and what it means to communicate and that helps people and enable them to think naturally. It’s time to make security personal. During our masterclasses or awareness sessions we get lots of employees who are uninvolved in the cyber world, I often share the real-life examples of how these cyber criminals or fraudsters are attacking everyone from big businesses to our friends and family members. And in these sessions as mentioned by Dave Gruber in one of his blogs I always ask everyone one question “What are you doing to help all of my friends, our children, and the rest of our community stay safe from cyberattacks?” As humans everything is personal to us and this is an important part of who we are as human beings, the things that matter to us literally become a part of our brains in a real concrete measurable way. If you are spreading awareness on basic Behavioural security measures or awareness across the organization, it is important you keep it personal. Rather than informing employees to follow the policies it will bring more adherence and impact if we make it personal. Let me show you some examples of how we in BT making security personal (Fig 19-21).



Did you shut your front door this morning?

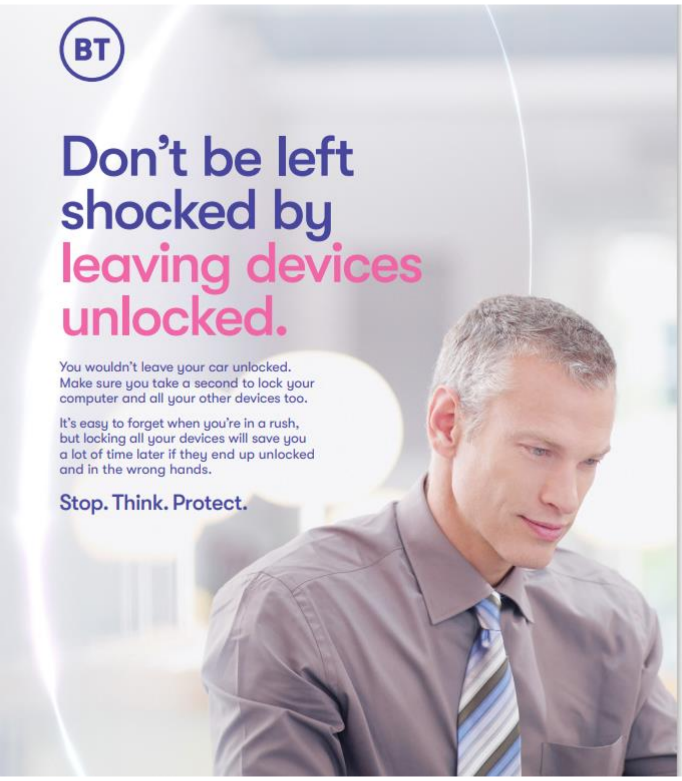
Of course you did,* because you don't want strangers stealing your stuff and threatening your family.

It's the same here: always check that doors and gates close behind you.

Help keep us all safe and secure.

Stop. Think. Protect.

Figure 19: The Door



BT

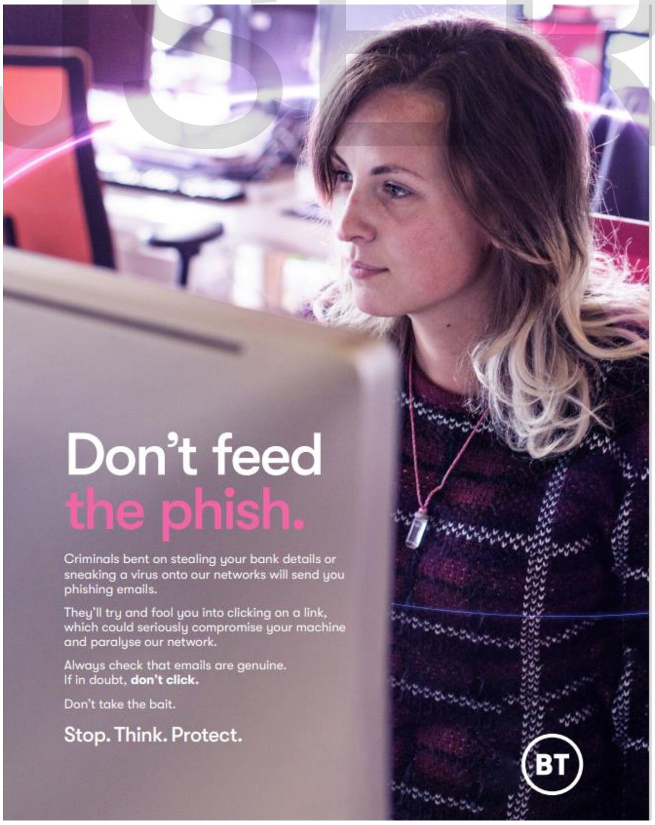
Don't be left shocked by leaving devices unlocked.

You wouldn't leave your car unlocked. Make sure you take a second to lock your computer and all your other devices too.

It's easy to forget when you're in a rush, but locking all your devices will save you a lot of time later if they end up unlocked and in the wrong hands.

Stop. Think. Protect.

Figure 20 : Leaving device unlocked



Don't feed the phish.

Criminals bent on stealing your bank details or sneaking a virus onto our networks will send you phishing emails.

They'll try and fool you into clicking on a link, which could seriously compromise your machine and paralyse our network.

Always check that emails are genuine. If in doubt, **don't click.**

Don't take the bait.

Stop. Think. Protect.

BT

Figure 21: Don't feed the Phish

5.6 Biriyani and Security

Security trainings are important for any industry including our one, but do people really complete these trainings properly or it’s more like a formality to them to complete? Reminding employees to stick to the rules feels like their parents telling them to eat healthy / homemade food regularly and avoid junk / restaurant food. You know they are right but anticipating that plain taste that awaits you simply puts you away. You decide to leave it for tomorrow, so much so that you never get to it.

Biriyani, on the other hand, are delicious and require not whatsoever to pamper in your cravings for them. Biriyani is an Indian dish made with highly seasoned rice, spices, clarified butter and meat. It does not require anyone to force you to eat a plate, may be two.

In our everyday lives we wish to do Biriyani tasks without giving it another thought. Things like storing confidential files on Dropbox or emailing them to our personal accounts you know, taking a little bite here and there. It is like we always tend to think as It's only for today', so that it gives us an assurance that it is so harmless, like an ease food. Quite often we realize later and sense bad that we bypassed a healthy food habit. At times we use our personal devices instead of a company-issued encrypted one, but at the end of the day who cares? Who will notice? If there is no histrionic impact on our health, a bite here or a bite there won't cause any harm.

Figure 22: The Great Indian Biriyani

But quite often one fine day we realize that it's not all healthy. The result of our laziness or lack of willpower eventually rears its ugly head when the doctor makes us stand on the scales and has a look at our blood pressure. To remind us our parents advise of wisdom is the doctor's warning of an unhealthy present and an unwelcoming future. This may sound very similar for the potential threats / challenges of the company's security.

We all must eat more healthy food and avoid junk foods e.g., Biriyani.

In our office we serve Biriyani 2 days per week and rest of the days we do serve like homemade meals and to no surprise on the days when we have Biriyani on our menu that gets over within 15 – 20 minutes where the rest of the days we get a lot of left over. The same things may observe with company’s security policies or trainings. We need a next generation chef who may come up with ways to make healthy foods more interesting, Same goes for us the data and security analysts to come up with more ideas which will help all employees maintaining their security diet.

We must try and brainstorm in making security more like Biriyani - effortless, even attractive, but keep it as healthy as a homemade food. I know it may not Sound as simple as it is in real. We must invest in serviceability studies to make sure that our security solutions are one of the easiest to use. This may involve learning a completely new cooking process. Now the big-time question is how to prepare healthy homemade food which tastes like Biriyani without letting everyone know. To achieve this we, the security professionals need each employees' support.

Organizations like ours are like one big family, we want to ensure all our family members stay healthy, otherwise when a single member gets sick, the whole family is at risk of getting sick as well, whether it be catching an infectious disease or adopting an unhealthy lifestyle. It's like having the slimmest, fittest family member refrain from adding biscuits to the grocery list in order not to tempt the lazy people. It's a team effort. For a company to stay healthy, everyone must keep a healthy lifestyle of eating healthy food regularly, even when it is not that pleasant.

The whole company needs to know that security is important for achieving its goals, just as we should all know that having healthy homemade foods will guarantee a healthy body. Employees contribute to the efficient operation of the business when they comply with security policies and complete their security trainings with full ownership. Not only does security ensure confidentiality and the integrity of information, but it also guarantees that the resources are available for employees to complete their primary tasks.

We need to realize that we contribute to security, and we can inflict serious damage on a company when we don't comply with security policies, no matter how insignificant or harmless they may seem. As employees, we are individually responsible for the organization’s exposure to security risks, just as we are responsible for exposing ourselves to illness. Our behaviour and daily regime significantly shape our quality of life, and our practices shape the quality of our business.

The health of the company is everyone's business. Let's all eat healthy homemade food while helping the security specialists to come up with better-tasting ones.

5.7 Increase the frequency of Security Trainings and Masterclasses

Most organizations mandate various security trainings for all their employees. With the increasing trend in Social engineering and phishing attacks, in addition to the trainings been made mandatory throughout the year, cyber security masterclasses have been introduced to provide additional support to all the employees. According to the research, the effect of these is concise. Now the question is, how often should cyber security training and masterclasses be repeated?

The increase in cyberattacks specially in recent days during the pandemic started to worry everyone, including the company employees. In addition to the increasing number of ransomware attacks, we face more and more sophisticated phishing attacks every day. Organizations should also change their cybersecurity environment, implement appropriate security training, and renew themselves. Every employee must be aware of current threats to be able to take effective measures through some masterclasses.

Studies show that phishing training increases cybersecurity awareness at a high rate in the short term, but their effects decrease over time. According to the results, while the training remains very effective for 4 months, they have almost no effect after 6 months. That’s why it’s critical to set up cybersecurity programs to repeat every 4 to 6 months.

October, which also known as National Cyber Security Awareness Month which has a different theme each year. Last year’s Awareness Month theme was “Do Your Part. #BeCyberSmart”. With this concept, they aim to increase the cyber awareness of companies and individuals. This reminds us that Cybersecurity Awareness Training Needs Regular Refreshment. Why so frequently? The knowledge and savvy that employees gain from security and phishing awareness training is forgotten over time. In a study of cybersecurity awareness training retention, test subjects went through a single training course. Researchers then retention tested them four, six, eight, ten and 12 months later. The findings concluded that the longer the test subjects went from the original training date, the worse their memory was of what they’d learned. The sweet spot for retention was at four months. Once the testers passed that mark, their retention dropped dramatically until their performance at ten months was the same as it was when they started the study.

The campaign aims to emphasize that cyber responsibility belongs to both the company and the employee. Both parties need to work hard for a proper cyber defense. Phishing training is perfect for this. Because today we receive thousands of phishing emails every day, which means that the emails managed to find us by circumventing various security measures. So, cyber security training and phishing simulations are essential to combat phishing emails. Also, it is critical that training is continuous. However, companies should adjust the training frequency so that they do not interrupt the work and do not bother the employees.

A single weak link in your company can cause your entire system to crash. You cannot be safe face to face until you have corrected all your weaknesses. That's why you should create a cybersecurity program that covers all levels of your company.

5.8 Recognition

One of the strongest influences on the security culture of an organization is employee recognition. Recognizing employees for their everyday contributions towards great behaviour on security being physical or cyber touches every aspect of the organization's environment and the overall employee experience. To keep employees motivated and contribute towards overall organizational security benefits and salary are not the only critical considerations of the employee experience and the overall company culture, recognitions are also major considerations as well. Let's look at six facets of workplace culture that help to make organizations more attractive to talent via employee recognition the first aspect is engagement a Gallup poll taken in 2017 reported a not so positive outlook on employee engagement and stated that as many as 51% of the

employee workforce is not actively engaged employees who receive strong recognition have been found to improve their work relativity and quality by 80%. Number two is improved leadership strong leaders that act as engaged mentors not only create a heightened sense of camaraderie but relationships between employees and leaders are improved especially when employees are recognized for their ongoing efforts. The third aspect is opportunity, providing employees with opportunities to grow and develop both personally and professionally is important recognition for achievements such as spotting a potential social engineering attack over social media platforms or proactively reporting spam messages or emails is a great motivator. Number four is success; employees want to feel as though they are part of a winning team and that their efforts for doing meaningful work are recognized when the company gets Awards or special mentions. Number five purpose give employees a reason for their presence and their contributions within the organization for them to feel connected many studies show that when people feel the purpose or reason for being or doing, they are more likely to be productive and happy. And finally, number six is wellbeing, organizations often focus solely on the physical aspects of workplace security culture however to create well-rounded employees' employers must also focus on the well-being that involves employees' emotions and social environments. Recognition is a tool not often seen as a key factor in workplace culture but to effectively make an impact on the organization and for the customers it should never be underestimated.

We must thanks to people who do something special and bring our values to life. This must include great behaviour showcased on the security aspect of the organization. A big bold Behavioural security culture needs a bigger bolder recognition scheme. Give a quick thank you on the recognition wall where others can see, like and comment on the recognition you give or receive.

"We must find time to stop and thank the people who make a difference in our lives."
John F. Kennedy

Figure 23: A quote from John F. Kennedy

Recognition is a keyway of celebrating the contribution that people are making right across the business to showcase great security behaviour and adherence to the culture. This must also include the efforts of any individual to spread awareness either by reporting security incidents or keeping all other co-workers informed on any potential security risks. We can say thank you and well done to people by sending them an email or e-card, we can also nominate them for a Role Model award (if available) or any other recognition program available within the organization. Within our organization we are continuously working to improve our reward framework to ensure we recognize every individual showcasing great behaviour in Security. We have dedicated badge as showing in the figure: 24 to recognize any of the instances like reporting Phishing emails, potential social engineering attacks etc.

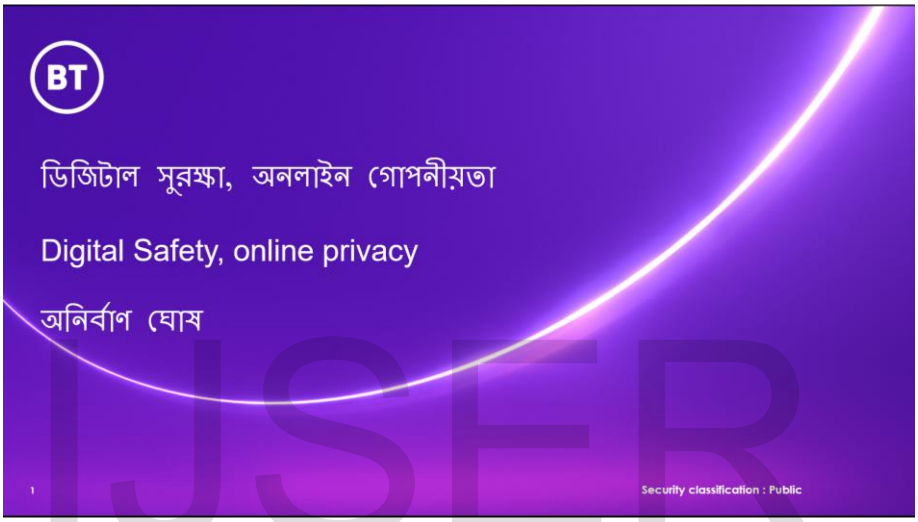
Thank you for being a security hero
Switch On Your Human Firewall
#humanfirewall

Figure 24: Security Hero appreciation badge

5.9 Make it a part of Social Responsibility

Corporate Social Responsibility (CSR) is about giving something back to society. It could be local, regional or on a global perspective. Our organization is very good at taking part in different activities to support different causes. In addition to helping and supporting the selected groups or projects, it is also an activity that help form good teams and generates pride among people taking part. Doing something that really matters, and to see the result is very satisfying. People working for the organization are allowed two working days per year for these kinds of activities. When you can turn a lazy Saturday morning into a fulfilling journey of empowering our next generation, that's when you know you've made it.

CSR is about making a real difference to the communities we operate in and to individuals there. In India we collaborate with different Non-Government Organizations to do our bit. During this research it's been observed how the young generations are interested in strengthening their Human Firewall to protect not only themselves but also their friends and family members from all these online frauds. Within our organization I have now been working with such and NGO named as "Transform Schools". Transform Schools is working in 67,000 government secondary schools to improve the learning outcomes of 2.4 million children across four States in India, increasing their transition to higher education and access to career opportunities. They do this by providing rigorously tested tools and training to teachers, students, governing bodies, and parents with the vision of "Every child and young person deserves the opportunity to realize their full potential and thrive." These are the perfect platform to spread awareness around cyber security for any organizations which indeed will create a great Corporate Social Responsibility story to tell. To start off I have created a quick 20 mins video-based masterclass for the school going girl students of 10th and 11th Standard based in Kolkata, India in their regional language "Bengali" the title slides as shown in figure 25.



ডিজিটাল সুরক্ষা, অনলাইন গোপনীয়তা

Digital Safety, online privacy

অনির্বাণ ঘোষ

1

Security classification : Public

Figure 25: The Digital Safety and Online Privacy Title slide

This was the very first attempt to this kind to spread awareness amongst school going children to help and support to keep the Human Firewall switched on. Let me take you through the content and the background of this initiative which is a recommendation for all organizations to follow as a part of their corporate social responsibility to ensure we create a safe and secure future for our coming generations specially the change in approach in the day-to-day life of everyone including our children due to COVID 19.

First, I must admit that We are going through some tough time, where we had to Move aside old-style fun and games for our children as well as ourselves. For all of us it's all about hash tag being connected all the time through phone apps, social media sites, online gaming AND shares likes tweets, and the list goes on and on. Technology is our middle name but there is such a thing as over exposure. One of those moments where all the parents are right. So, while we and our children enjoy the freedom let's also keep an eye on the serious dangers hiding in the vast web of communication. It sounds scary but with just a few rules we all can stay safe online.

Rule Number one do not accept requests from unknown people, the first thing our mummy has taught us since we were little which is don't talk to strangers. The same rule applies online as simple as that. Unknown online entities posing as friends may want to chat with you or share emails, but just hold on for a second and think why an unknown person would suddenly want to be friends with you. If you have ever accepted any such requests in the past then it’s time to remove them from the list, also do not share your personal information with anyone online until and unless you are sure about the person. And never ever meet up with them in real life, this may turn out to be a personal security issue if the person has bad intent.

Rule Number 2 be mindful of photo sharing. It's the age of Facebook, Instagram, Snapchat, WhatsApp, and YouTube. Publishing posts, pictures or videos is the language we all are talking. Afterall who wouldn't want to be the coolest person of millennial town? But always remember to keep your privacy setting to Friends ONLY, we do not want the whole world to know our every move. Also remember putting up loads of your personal information on the Internet can turn into an invitation for negative entities to use and more importantly to misuse it Like - like creating fake online accounts using your name and Photo, Use your details for illegal activities and fake money transactions all this using your identity.

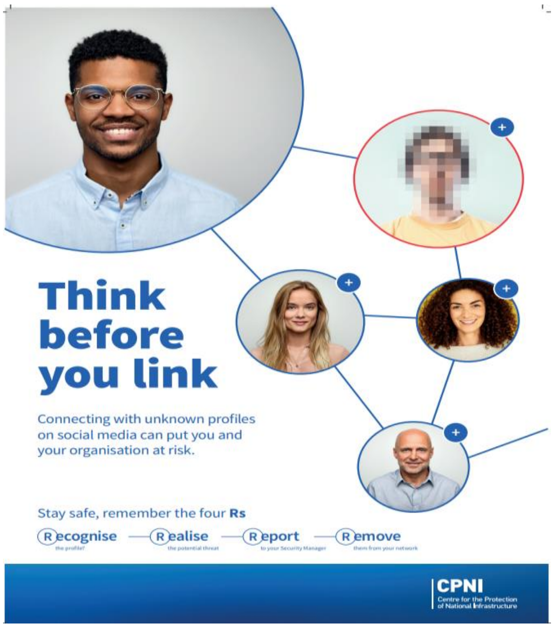
Rule Number 3 - Safeguard your EMAIL AND social Media apps. Enable two factor authentications like after login with your ID and Password enable a Pin or OTP to be validated This will ensure you are safe with all your accounts. Always enable notification and select right alerts and configure privacy policy as only share with friends while sharing any information.

Rule number 4 and the most important one - beware of cyber bullies. When our parents were kids bullies only roamed in the school corridors. Well today they are also on our computers and phones. cyberbullies are all those nasty faceless guys who will take offence to even a simple post and use abusive offensive language to put you down. This is a real risk for us and our children as being online is a part of all our life now a days. So, what do you do, or you teach to your children if anyone you know face this type of situation? First, do not be afraid, Second Just blocked them and ask to report them to parents / teachers/ your elder sibling with whoever they are comfortable with. for good every mobile app or social media that has an easy to operate feature for reporting cyber bullies, so use the report option to report any Post/ Comment/Photo / Video after which it's the company's job to act.

The above content made real difference in the kids' day to day life and the feedback which been received was simply fantastic. The one thing which everyone of us must start spreading across the world is **When you post online, you post to the world!!! This is important.**

5.10 Think Before You Link

In BT we do work together with Centre for the Protection of National Infrastructure who are the UK government's National Technical Authority for physical and personnel protective security. One of their recent campaigns which we did promoted across the organization is "Think Before You Link" as per Figure: 26. This is designed to report suspicious profiles and remove them from their official or personal / private network. Criminals and hostile actors may act anonymously or dishonestly online to connect with people who have access to valuable and sensitive information. They often do this by posing as recruiters or talent agents who will approach individuals with enticing opportunities, when their real intent is to gather as much information as possible from the target. The consequences of engaging with these profiles can damage individual careers, as well as the interests of your organization, and the interests of UK national security and prosperity. This guidance provides practical advice on how to identify them, how to respond, and how to minimize the risk of being targeted in the first instance.



Think before you link

Connecting with unknown profiles on social media can put you and your organisation at risk.

Stay safe, remember the four **Rs**

Recognise the profile? — Realise the potential threat — Report to your Security Manager — Remove them from your network

CPNI
Centre for the Protection of National Infrastructure

Figure 26: Think before you link

As per the research done by CPNI The Five Es Behaviour Change Framework is key to the success of every campaign and is made up of five principles as shown in Figure 27.

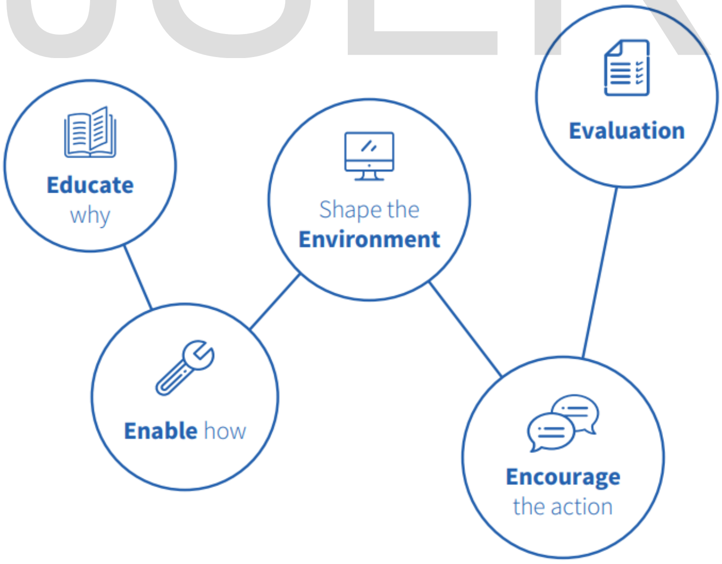
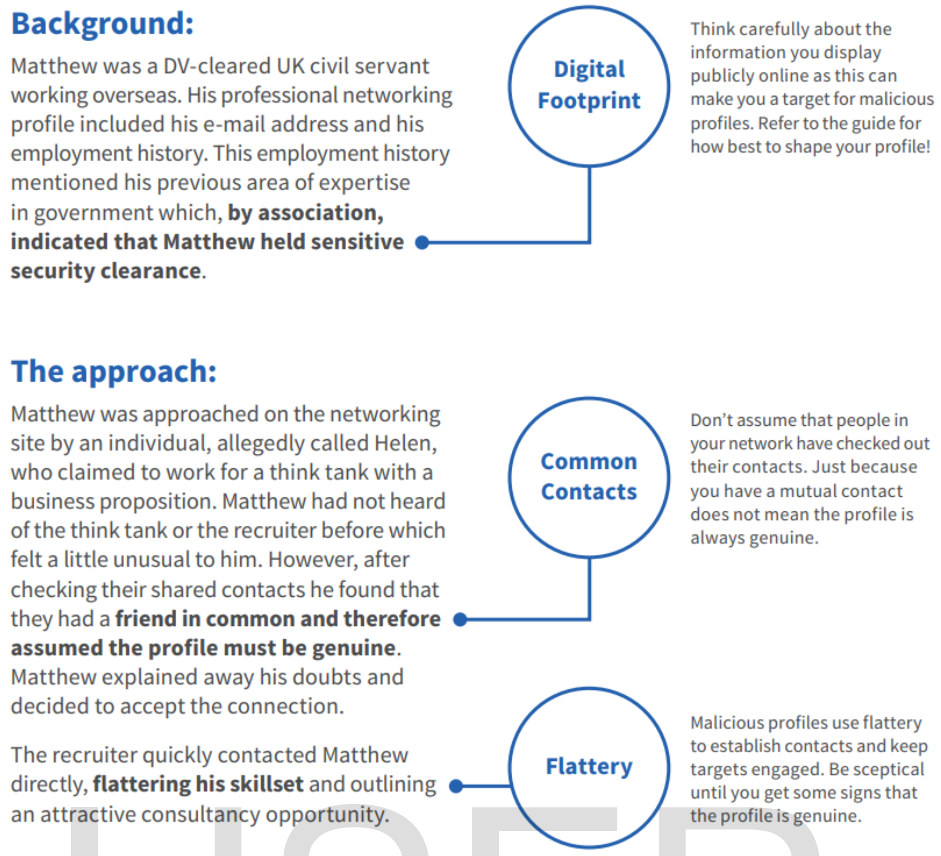


Figure 27: The Five Principles

- **Educate -** People are more likely to engage in behaviour if they understand why it is important to do so. Educating is about helping staff to understand the nature of the threat, and why this poses at risk them, the organisation and national security.

- **Enable -** To behave in the desired way, staff need the necessary resources. In this context, they need clear, concise instructions on how to identify a malicious profile and what to do when they are approached by one.
- **Shape the Environment -** Environmental cues can make it easier to do the right action, so it's important to shape the environment and ensure that the desired behaviours are as easy as possible for staff to do. In this campaign, this might involve re-shaping reporting mechanisms so that they are streamlined and easy to use.
- **Encourage the action -** Staff need feedback to help reinforce the desired behaviour and discourage the undesired one. If staff receive little or no meaningful feedback in response to their reporting, they may feel ignored and associate this behaviour with a negative experience. This could make them less likely to report again.
- **Evaluation-** Like all change initiatives, assessing the impact of your campaign is an important step. Demonstrating the impact of the work will help raise support for future initiatives.

Let's investigate one of the Case Study done by CPNI: "Matthew" – Figure 28 – 30.



Background:

Matthew was a DV-cleared UK civil servant working overseas. His professional networking profile included his e-mail address and his employment history. This employment history mentioned his previous area of expertise in government which, **by association, indicated that Matthew held sensitive security clearance**.

Digital Footprint

Think carefully about the information you display publicly online as this can make you a target for malicious profiles. Refer to the guide for how best to shape your profile!

The approach:

Matthew was approached on the networking site by an individual, allegedly called Helen, who claimed to work for a think tank with a business proposition. Matthew had not heard of the think tank or the recruiter before which felt a little unusual to him. However, after checking their shared contacts he found that they had a **friend in common and therefore assumed the profile must be genuine**. Matthew explained away his doubts and decided to accept the connection.

Common Contacts

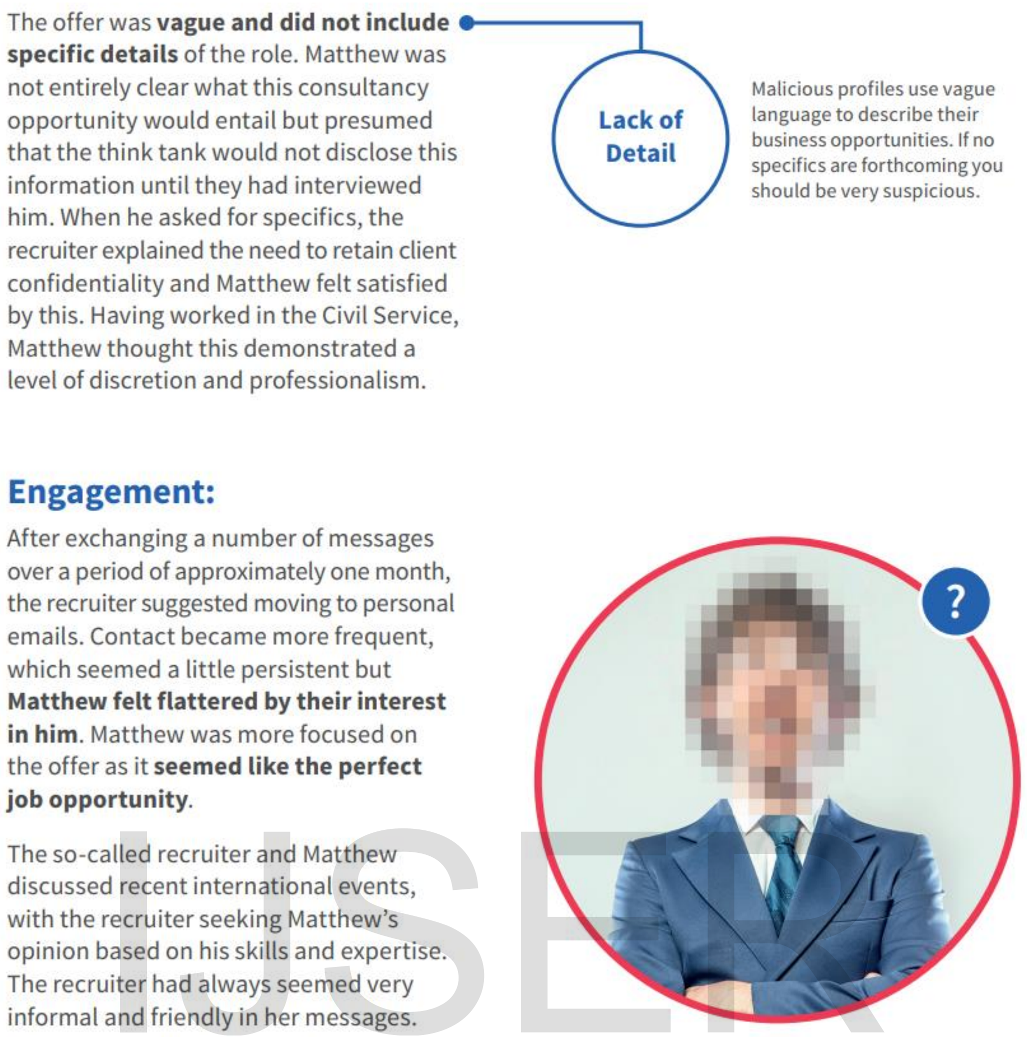
Don't assume that people in your network have checked out their contacts. Just because you have a mutual contact does not mean the profile is always genuine.

The recruiter quickly contacted Matthew directly, **flattering his skillset** and outlining an attractive consultancy opportunity.

Flattery

Malicious profiles use flattery to establish contacts and keep targets engaged. Be sceptical until you get some signs that the profile is genuine.

Figure 28: Case Study1



The offer was **vague and did not include specific details** of the role. Matthew was not entirely clear what this consultancy opportunity would entail but presumed that the think tank would not disclose this information until they had interviewed him. When he asked for specifics, the recruiter explained the need to retain client confidentiality and Matthew felt satisfied by this. Having worked in the Civil Service, Matthew thought this demonstrated a level of discretion and professionalism.

Lack of Detail

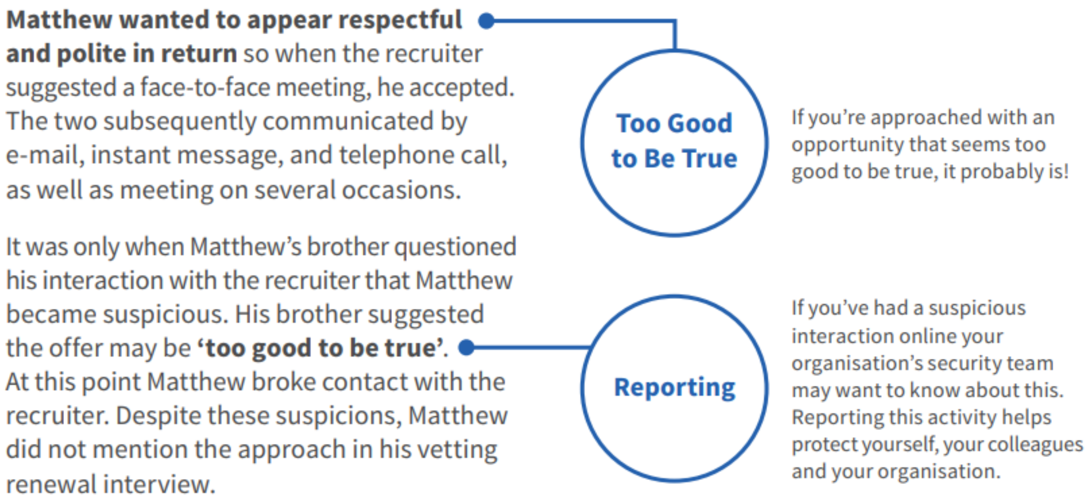
Malicious profiles use vague language to describe their business opportunities. If no specifics are forthcoming you should be very suspicious.

Engagement:

After exchanging a number of messages over a period of approximately one month, the recruiter suggested moving to personal emails. Contact became more frequent, which seemed a little persistent but **Matthew felt flattered by their interest in him**. Matthew was more focused on the offer as it **seemed like the perfect job opportunity**.

The so-called recruiter and Matthew discussed recent international events, with the recruiter seeking Matthew's opinion based on his skills and expertise. The recruiter had always seemed very informal and friendly in her messages.

Figure 29: Case Study2



Matthew wanted to appear respectful and polite in return so when the recruiter suggested a face-to-face meeting, he accepted. The two subsequently communicated by e-mail, instant message, and telephone call, as well as meeting on several occasions.

It was only when Matthew's brother questioned his interaction with the recruiter that Matthew became suspicious. His brother suggested the offer may be **'too good to be true'**. At this point Matthew broke contact with the recruiter. Despite these suspicions, Matthew did not mention the approach in his vetting renewal interview.

Too Good to Be True

If you're approached with an opportunity that seems too good to be true, it probably is!

Reporting

If you've had a suspicious interaction online your organisation's security team may want to know about this. Reporting this activity helps protect yourself, your colleagues and your organisation.

Figure 30: Case Study3

To stay safe from being one of the victims we must Memorise the four Rs to protect ourselves against malicious profiles per Figure 31.

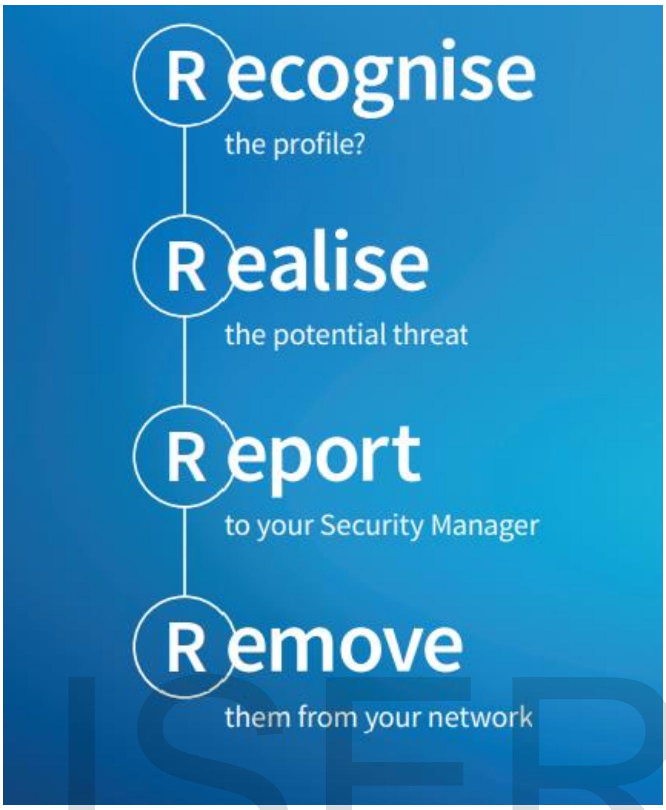


Figure 31: Four Rs

1. **Recognise the profile? -** When a new connection adds you or gets in touch on social networks check to see if you recognise them first. If you do not recognise them watch out for signs that you can associate with fake or malicious profiles. We all know that things on the internet are not always as good as they seem.
   For example, when shopping online you might find what looks like a great deal, but a quick look around the web can help you unmask a potential scam. The same is true of opportunities on social and professional networking sites. If you've been contacted by a profile you don't recognise.
2. **Realise the potential threat -** You may realise the threat from the way the profile looks and the kind of personal and professional information it lists. But if not, the next signs you should look for are related to the way the profile engages with you.

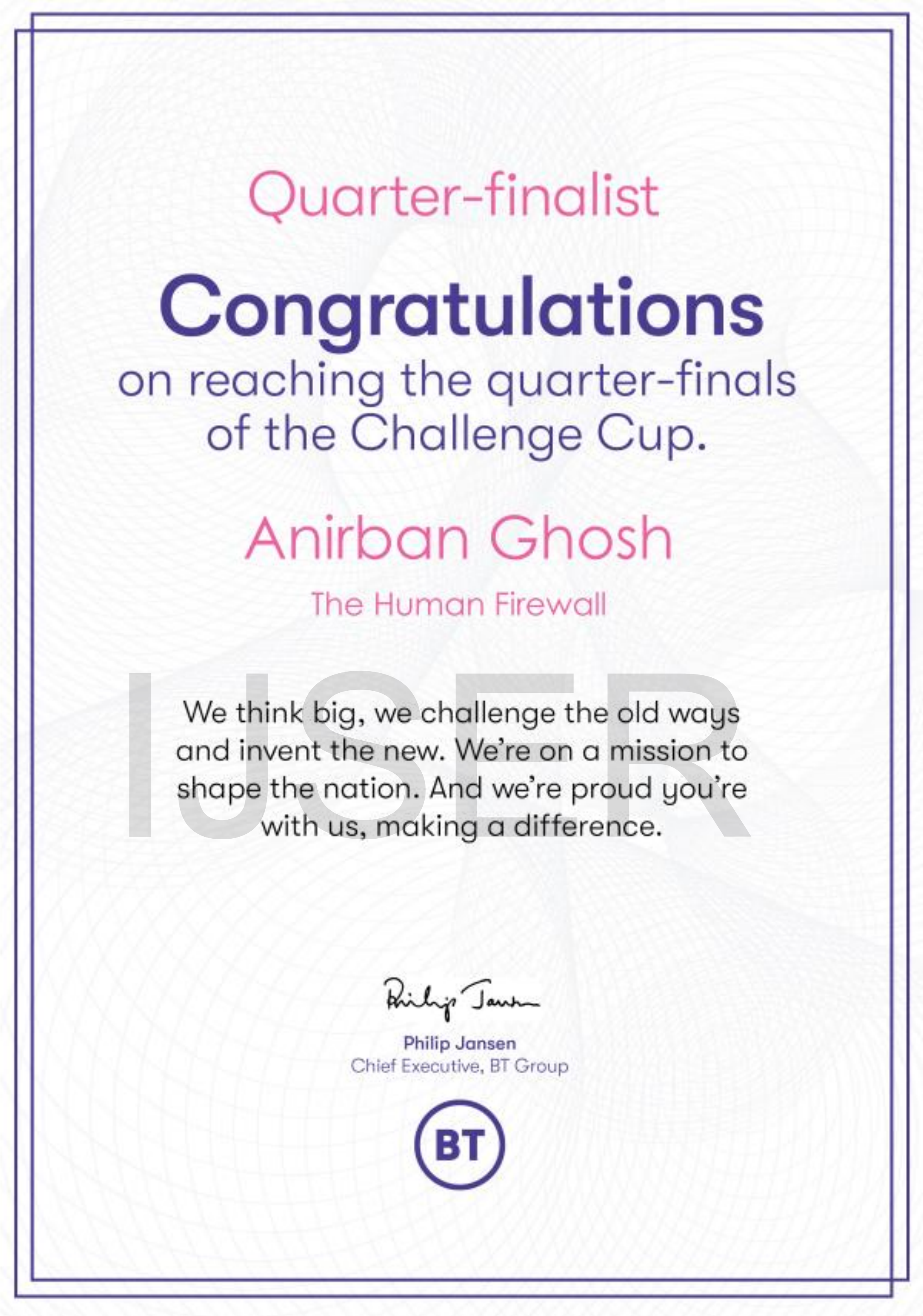
3. **Report to your Security Manager -** Once you realise that you might have been contacted by a malicious profile, reporting them to your Security Manager is the best way to protect yourself and others. All platforms provide robust reporting mechanisms for suspicious profiles or content and you should report through these channels as well as reporting internally.
4. **Remove them from your network -** Keeping malicious profiles in your network adds legitimacy to them and puts your colleagues, organisation, and other contacts at risk. Encourage your trusted friends and colleagues to also remove these profiles if they have connected too.

There are two audiences potentially viewing your profile – genuine professional contacts who support your credibility and raise your profile, and those who are out to exploit you and your organisation. When managing your profile, you want to provide enough relevant information to your genuine contacts without giving away so much detail that it makes you vulnerable to targeting by malicious profiles. Think about what is the lowest level of detail that you need to provide for your profile to promote you properly to friendly audiences. What is the relevant information to potential talent hunters or recruiters? Does your profile give away unnecessary detail? To protect yourself and your organisation from malicious profiles, start with making your online presence secure. And, when contacted by someone new, always remember the four Rs

5.11 Restrictions of Applicability & Probability for Future Research

The finding of this thesis, and the efficiency of any training program created to incorporate this research paper depends largely on the ability of previous research done on the human phycology and its relatable impact on any potential cyber or social engineering attacks. This research and the relevant hard work brought significant improvement on the overall Behavioural security management of BT; the same techniques may not be effective against all organizations. With that said, more research is required in this area.

If a means of measuring an individual's vulnerability to social engineering can be developed, then a study that verifies the effectiveness of this type of training when applied to social engineering would add validity to this study.



Quarter-finalist

Congratulations

on reaching the quarter-finals
of the Challenge Cup.

Anirban Ghosh

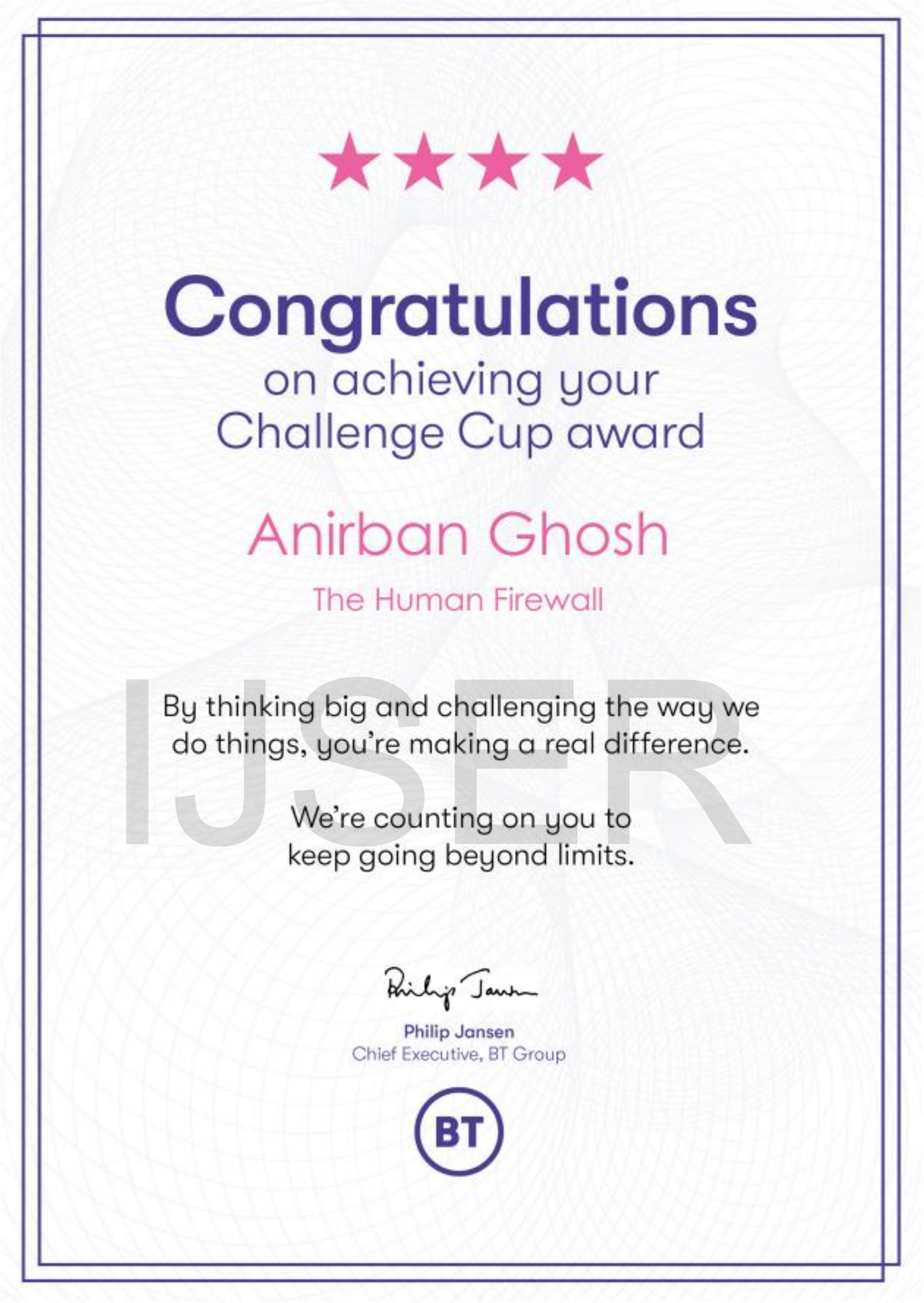
The Human Firewall

We think big, we challenge the old ways
and invent the new. We're on a mission to
shape the nation. And we're proud you're
with us, making a difference.

Philip Jansen
Chief Executive, BT Group

BT

Figure 32: The Quarter Final award



★★★★

Congratulations

on achieving your
Challenge Cup award

Anirban Ghosh

The Human Firewall

By thinking big and challenging the way we
do things, you're making a real difference.

We're counting on you to
keep going beyond limits.

Philip Jansen

Philip Jansen
Chief Executive, BT Group

BT

Figure 33: The completion award

Reference list

Books

Foreword, W. P.-, Hadnagy, C., Chandler, A. T., & Gildan Media. (2018). Social Engineering: The Art of Human Hacking. Gildan Media.

May, R. (2018). The Human Firewall: Cybersecurity is not just an IT problem (2nd ed.). Independently published.

Publishing, G. I. T. (2016). The Psychology of Information Security. It Governance Publishing.

Ustaran, E. (2021). European Data Protection Law and Practice (2nd ed.). International Association of Privacy Professionals.

Hadnagy, C., Fincher, M., & Dreeke, R. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails (1st ed.). Wiley.

Foreword, W. P.-, Hadnagy, C., Chandler, A. T., & Gildan Media. (2020). Social Engineering: The Art of Human Hacking. Gildan Media.

Thesis

Scheeres, Jamison W., "Establishing the Human Firewall: Reducing an Individual's Vulnerability to Social Engineering Attacks" (2008). Theses and Dissertations. 2790. https://scholar.afit.edu/etd/2790

Bulleit, William & Schmidt, Jon & Alvi, Irfan & Nelson, Erik & Rodriguez-Nikl, Tonatiuh. (2014). Philosophy of Engineering: What It Is and Why It Matters. Journal of Professional

Issues in Engineering Education and Practice. 141. 02514003. 10.1061/(ASCE)EI.1943-5541.0000205.

Blogs / News Articles / Campaigns

Hacking Human Psychology: Understanding Social Engineering Hacks | Blog. (2019, November 21). Relativity. https://www.relativity.com/blog/hacking-human-psychology-understanding-social-engineering/

Think Before You Link. (2021, July 6). CPNI. https://www.cpni.gov.uk/security-campaigns/think-you-link

S. (2020, November 17). Whaling: Why Go After Minnows When You Can Catch a Big Phish? Social-Engineer, LLC. https://www.social-engineer.com/whaling-why-go-after-minnows-when-you-can-catch-a-big-phish/

Mayhew, J. (2020, November 12). Benefits of VR for Developing Soft Skills. Virtualspeech.Com. https://virtualspeech.com/blog/benefits-vr-soft-skills-training

F. (2021, February 5). Why Human Error is #1 Cyber Security Threat to Businesses in 2021 | Firewall Security Company India. Firewall Security Company India | Complete Firewall Security Solutions Provider Company in India. https://firewall.firm.in/why-human-error-is-1-cyber-security-threat-to-businesses-in-2021/

The Impact of Social Media: Is it Irreplaceable? (2019, July 26). Knowledge@Wharton. https://knowledge.wharton.upenn.edu/article/impact-of-social-media/

Moramarco, S. (2018, October 10). How to Create a Human Firewall: Top 7 Elements Required for Success in 2018. Security Boulevard. https://securityboulevard.com/2018/10/how-to-create-a-human-firewall-top-7-elements-required-for-success-in-2018/

The Hacker News. (2021, April 2). Why Human Error is #1 Cyber Security Threat to Businesses in 2021. Magzter.Inc. https://www.magzter.com/news/688/1966/022021/c9gkb

Appelbaum, Steven & Profka, Edmiela & Depta, Aleksandra & Petrynski, Bartosz. (2018). Impact of business model change on organizational success. Industrial and Commercial Training. 50. 10.1108/ICT-07-2017-0058.

Aiken, M. (2016). The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behaviour Changes Online. United Kingdom: John Murray Press.

Demakis, A. R., Demakis, A. R., Demakis, A. R., Demakis, A. R., & Demakis, A. R. (2021, August 12). Security Archives. Demakis Technologies. https://demakistech.com/category/security/

Demakis, R. (2021, March 11). Social Engineering - Demakis Technologies - IT Solutions. Demakis Technologies. https://demakistech.com/social-engineering/

Elmore Insurance Brokers. (2020, November 17). Human Firewall. https://elmorebrokers.com/review/cyber-security/human-firewall/

Kanade, V. (2021, August 4). What Is Social Engineering? Definition, Types, Techniques of Attacks, Impact, and Trends. Toolbox. https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-social-engineering/

Riva, Giuseppe. (2012). What is Positive Technology and its impact on CyberPsychology.. Studies in health technology and informatics. 181. 37-41. 10.3233/978-1-61499-121-2-37.

3 steps to boost your digital safety while working from home. (2020, May 25). World Economic Forum. https://www.weforum.org/agenda/2020/05/3-steps-to-boost-your-digital-safety-while-working-from-home/

Benton, S. (n.d.). Remote working security guide â“ the human firewall. BTBusiness. Retrieved September 12, 2021, from https://business.bt.com/remote-working-security/

Davison, A. (2021, March 3). CISOs must step up as cybersecurity takes centre stage. IT-Online. https://it-online.co.za/2021/03/03/cisos-must-step-up-as-cybersecurity-takes-centre-stage/

INTERPOL | The International Criminal Police Organization. (n.d.). CISOs under the Spotlight - Interpol. Retrieved September 12, 2021, from https://www.interpol.int/

Moramarco, S. (2018, October 10). How to create a human firewall: Top 7 elements required for success. Infosec Resources. https://resources.infosecinstitute.com/topic/how-to-create-a-human-firewall-top-7-elements-required-for-success-in-2018/

Benton, S. (n.d.). Turn on the human firewall. Turning on the Human Firewall. Retrieved September 12, 2021, from https://www.globalservices.bt.com/en/insights/blogs/turning-on-the-human-firewall

Gaming consoles and platforms - Home Life - Skills for Tomorrow | BT. (n.d.). Gaming Console. Retrieved September 12, 2021, from https://www.bt.com/skillsfortomorrow/home-life/gaming-consoles-and-platforms

Bellasio, Jacopo, Erik Silfversten, Eireann Leverett, Anna Knack, Fiona Quimbre, Emma Louise Blondes, Marina Favaro, and Giacomo Persi Paoli, The Future of Cybercrime in Light of

Technology Developments. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA137-1.html.

Parent controls - entertainment and search engines - Home Life - Skills for Tomorrow | BT. (n.d.). Parent Controls. Retrieved September 12, 2021, from https://www.bt.com/skillsfortomorrow/home-life/parent-controls-entertainment-and-search-engines

Security, E. (2018, November 21). What makes a security company a "one-stop-shop"? EPS Security. https://www.epssecurity.com/news/business-security/what-makes-a-security-company-a-one-stop-shop/

topic - Dictionary Definition. (n.d.). Vocabulary.Com. Retrieved September 12, 2021, from https://www.vocabulary.com/dictionary/topic#:%7E:text=If%20something%20is%20a%20%22hot,of%20topics%20with%20other%20guests.

K. (2020, December 23). How Often Should Cyber Security Training Be Repeated? Phishing.Org.Uk. https://www.phishing.org.uk/2020/12/23/how-often-should-cyber-%e2%80%8b%e2%80%8bsecurity-training-be-repeated/

M. (2021, August 13). How Often Should Businesses Run Cybersecurity Awareness Training? ID Agent. https://www.idagent.com/blog/how-often-should-businesses-run-cybersecurity-awareness-training/#:%7E:text=Usenix%20found%20that%20the%20knowledge,training%20is%20forgotten%20over%20time.

Spotlight 2020–2021. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/corporate_pubs/CPA1150-1.html.

McNeal, A. (2021, May 20). How Often Should Businesses Run Cybersecurity Awareness Training? Security Boulevard. https://securityboulevard.com/2021/05/how-often-should-businesses-run-cybersecurity-awareness-training/

Young, K. S. (1998). Caught in the Net: How to Recognize the Signs of Internet Addiction--And a Winning Strategy for Recovery (1st ed.). Wiley.

V., P. (2016). INTERNET ADDICTION AND CYBER CRIME ENGAGEMENT OF UNDERGRADUATE STUDENTS. INTERNET ADDICTION AND CYBER CRIME ENGAGEMENT OF UNDERGRADUATE STUDENTS, 53(3), 6–7. http://srkvcoe.org/JERE/journaladmin/journals/Vol._53_Issue._33869.pdf

PricewaterhouseCoopers. (n.d.). How virtual reality is redefining soft skills training. PwC. Retrieved September 12, 2021, from https://www.pwc.com/us/en/tech-effect/emerging-tech/virtual-reality-study.html

Technology, T. (2021, May 25). How Often Should Businesses Run Cybersecurity Awareness Training? Tecbound Technology. https://www.tecbound.com/how-often-should-businesses-run-cybersecurity-awareness-training/

Gruber, D. (2019, October 29). It Time to Make Cybersecurity Personal: Here’s How. Esg-Global. https://www.esg-global.com/blog/-it-time-to-make-cyber-security-personal-heres-how

Images

AF archive / Alamy Stock Photo. (2004, May 12). SCENE WITH TROJAN HORSE TROY (2004) - Image ID: BPMM03 [Photograph]. SCENE WITH TROJAN HORSE TROY (2004).

https://www.alamy.com/stock-photo-scene-with-trojan-horse-troy-2004-31187523.html?pv=1&stamp=2&imageid=CACB4002-722A-41E4-AFE5-210B306AEF6A&p=89858&n=0&orientation=0&pn=1&searchtype=0&IsFromSearch=1&srch=foo%3dbar%26st%3d0%26pn%3d1%26ps%3d100%26sortby%3d2%26resultview%3dsortbyPopular%26npgs%3d0%26qt%3dtrojan%2520horse%26qt_raw%3dtrojan%2520horse%26lic%3d3%26mr%3d0%26pr%3d0%26ot%3d0%26creative%3d%26ag%3d0%26hc%3d0%26pc%3d%26blackwhite%3d%26cutout%3d%26tbar%3d1%26et%3d0x000000000000000000000%26vp%3d0%26loc%3d0%26imgt%3d0%26dtfr%3d%26dtto%3d%26size%3d0xFF%26archive%3d1%26groupid%3d%26pseudoid%3d%26a%3d%26cdid%3d%26cdsrt%3d%26name%3d%26qn%3d%26apalib%3d%26apalic%3d%26lightbox%3d%26gname%3d%26gtype%3d%26xstx%3d0%26simid%3d%26saveQry%3d%26editorial%3d1%26nu%3d%26t%3d%26edoptin%3d%26customgeoip%3d%26cap%3d1%26cbstore%3d1%26vd%3d0%26lb%3d%26fi%3d2%26edrf%3d%26ispremium%3d1%26flip%3d0%26pl%3d

idagent. (2020, June 15). 10 Alarming Statistics About Phishing [Photograph]. Phishing. https://www.idagent.com/blog/10-alarming-statistics-about-phishing-in-2020/

Pixabay. (2015, February 8). person-walking-pipeline-tube-steel-731319 [Photograph]. https://pixabay.com/photos/person-walking-pipeline-tube-steel-731319/

purplesec. (2021, August 9). What Is Vishing? [Photograph]. The Vishing Process. https://purplesec.us/wp-content/uploads/2020/08/what-is-vishing.png

shutterstock. (2019, September 1). BEC Attacks using Malicious Email Accounts [Photograph]. Shutterstock_1451268602. https://cisomag.eccouncil.org/wp-content/uploads/2019/09/shutterstock_1451268602.jpg community.microfocus.com. (2021, May 10). You Can Have Security Without Privacy. . . But You Cannot Have Privacy without Security! [Photograph]. The Quote on Security by ICO. https://community.microfocus.com/resized-image/__size/400x400/__key/communityserver-wikis-components-files/00-00-00-02-94/23649iFB551E67070E5942.png

DOBRAN, B. O. J. A. N. A. (2019, February 26). how Spear phishing works [Photograph]. The Spear Phishing Process. https://phoenixnap.com/blog/wp-content/uploads/2021/08/how-spear-phishing-works.png

DQINDIA ONLINE. (2019, November 27). SMS Fraud [Photograph]. Sample Smishing Attack. https://www.dqindia.com/wp-content/uploads/2019/11/SMS-Fraud.jpg

Facebook. (n.d.). Workplace by Facebook [Photograph]. The Workplace by Facebook. https://static.xx.fbcdn.net/rsrc.php/v3/yP/r/IfjJf7QoAfT.png

spambrella. (n.d.). Whaling [Photograph]. The Whaling Attack. https://www.spambrella.com/wp-content/uploads/2019/12/whaling-attacks-300x151.png

nnit.com. (n.d.). NNIT Cybersecurity Training in Virtual Reality [Photograph]. Sample Virtual Reality Security Training. https://www.nnit.com/media/1xzomlth/screenshot_vr_infosecurity.jpg?width=1920&format=webp

onmanorama.com. (2018, June 30). Hyderabadi dum biriyani . . . Read more at: https://www.onmanorama.com/food/recipe/2018/06/30/hyderabadi-dum-biryani-biriyani-recipe-rice-dishes.html [Photograph]. The Great Indian Biriyani. https://www.onmanorama.com/content/dam/mm/en/food/in-season/Ramzan/Images/hyderabadi-dum-biryani.jpg.transform/onm-articleimage/image.jpg

Videos

Psychological Manipulation Vs Healthy Social Influence. (2020, February 23). [Video]. YouTube. https://www.youtube.com/watch?v=3HNjG92FpP8

YouTube. (n.d.). Youtube.com. Retrieved September 11, 2021, from https://www.youtube.com/

Shodhganga@INFLIBNET: Browsing Shodhganga. (n.d.). Shodhganga. Retrieved September 11, 2021, from https://shodhganga.inflibnet.ac.in/browse?type=title

Howland, L. (2020, January 30). Video: Cyber Chat – Episode 1 – Creating a strong human firewall. Ramsac. https://www.ramsac.com/blog/video-cyber-chat-episode-1-creating-a-strong-human-firewall/

Making Security Personal with Personas. (2021, June 9). [Video]. YouTube. https://www.youtube.com/watch?v=TOuXEWhcI-o&t=62s