May 2018

THE CYBERFISH

Photo credit: Awesome Arts

by Berta

AT THE CYBERFISH, WE HAVE A MISSION...

We are dedicated to teach people to defend themselves, their businesses and their families in the digital realm. We know that technology alone won't be able to stop cyber-crime. People will. But only if we help them shift to a digitally aware-mindset – fully conscious of the risks, the threats and equipped to deal with potential incidents before they even arise.
We are here to hammer home the importance of businesses making a cultural shift, from the mailroom to the boardroom.
We provide advice, tips and strategies on how best to make it happen.

Inside the Issue

THE PSYCHOLOGY OF A CRISIS

by Berta

Incident simulation exercises, or wargames are widely accepted and used tools designed to visualise the actual situation that takes place in the event of a cyber attack or data breach. By wargaming, information security teams and in general, leadership teams can attempt to foresee the possible interaction between corporate defences (blue team) and a simulated attack (red team) an adversary would carry out.

When this exercise is done concentrating on the adversary activities and focusing on the digital defences of an organisation, mostly the red team is trying to penetrate the IT systems of an organisation, using well known vulnerabilities and tools, techniques, procedures of what an enemy or cyber criminal would use. This is a fairly technical exercise that aims to identify gaps in the organisation's systems and on-line defences.

Whilst the output of these exercises are indispensable to the technical team, the strategic management will most of the time find the results of a penetration test too technical to draw final conclusions or make far reaching changes to the strategic digital posture of the organisation.

However, an attack simulation exercise provides an opportunity for leaders from other business units to participate and understand the full implications of a potential data breach using different attack use case scenarios.

Participating in a simulation or tabletop exercise allows non-technical people to address 'what if' questions and overview risks that would normally be addressed with a view to the development of contingency plans, allocation of necessary resources and creating internal synergies between stakeholders.

Understanding the adversary's behaviour and clarifying the biases and vulnerabilities of the organisation are a good base to be better able to anticipate events and most importantly, avoid surprises. Revising the decision making process shapes the best courses of action and helps individuals from across different units, such as operations, finance, legal, customer services, compliance, PR and IT work together.

Using the results of the wargaming outcomes is a powerful tool to create and promote digital risk awareness within the organisation, especially from the perspective of strategic leadership. It allows corrective measures to be taken and the recommendations can form part of budget making and approval process.

Involving a cyber psychologist in the exercise allows teams to look at team dynamics, social skills, communication skills of team members and help address future crisis situations with recommendations in terms of how team members can develop their performance when under stress.

Introducing the perspective of the adversary's behaviour in the course of social engineering attacks helps participants learn first hand what techniques attackers may use to convince others via email, phone call or other means.

An objective observer can help take a step back and look at the situation with a fresh perspective in order to testing the 'human factor': whether the staff's response will be adequate and if not, what can be done to improve these.

Fundamentally having a behaviourist insight helps team members gather an objective assessment of their interactions and recommendations with a view to personal development or improving team dynamics.

CYBER PSYCHOLOGY

by Lauren

This month I join The CyberFish team to further provide an insight into the psychology behind Cybersecurity. I studied Cyberpsychology as part of my degree in Psychology which ultimately sparked my interest in raising the awareness of how easy it is to compromise individual's and companies' online activities. My specialism includes Digital Addiction, Online Predators, Trust and relationships online and Social Engineering.

Mann (2008) defines Social Engineering as 'To manipulate people, by deception, into giving out information, or performing an action'. In October 2015, five hackers using the alias 'Crackas With Attitude' (CWA) successfully socially engineered and hacked into the personal AOL email account of the Central Intelligence Agency's (CIA) Director, John Brennan. This article will outline the psychological techniques that the hackers used to successfully administer the attack and humiliate their target.
Schneier (2006) argues that people misperceive risk in a number of ways, one being the underestimating of risks they are responsible for whilst overestimating risks outside of their control. For instance, Brennan could downplay the risk of his personal email being hacked, compared to his work email which is protected by the CIA's security. Perhaps if Brennan was more educated about the risks of storing sensitive documents on a personal email account, he may have been motivated to protect himself from potential risks – otherwise known as the Protection Motivation Theory (Rogers, 1975). Moreover, it is noted that people are more likely to ignore warnings about potential dangers if they consider themselves effective at minimising the effects of privacy violations. So, as Director of the CIA, it could be assumed that Brennan exhibited ignorance regarding his security.

Once the CWA learned that Brennan was a Verizon customer, they used a vishing attack – defined as when an attacker uses a phone to extract information from a target with the intention to cause harm. One of the attackers posed as a Verizon worker and called a Verizon employee help line, confidently reciting a fictitious employee number to validate his identity. Tversky and Kahneman (1975) theorized the term of a heuristic as when an individual uses a mental shortcut to create a snap judgement. Coupled with the heuristic that they must be a real employee as they have an employee number, this technique is effective as the familiarity of a colleague is more likely to encourage the real Verizon employee to trust him. The Uncertainty Reduction Theory suggests that reciprocal disclosure, in that the more certain about others behaviour (e.g. a colleague), the more you trust and more likely you are to disclose to this person. An alternative explanation for this behaviour is that the operator had a fear of potential embarrassment by not trusting a fellow employee.

The real Verizon employee could be termed as an 'unintentional insider', who are defined as individuals working for the target company who unwittingly facilitate outside attacks. It id said that people have a tendency to help others who are perceived to be in the company because they fear reprimand. The Integrity and Consistency trigger is a theory that states people have a tendency to believe that others are expressing their true attitudes when they make a statement (Gragg, 2003). This tendency is also said to be based on their own honesty in voicing thoughts. The hacker then asked for help, using the pretext that his system was down and had a customer on scheduled call back. This created a sense of urgency for the hacker, confirming Kearney and Kruger's (2016) theory that enabled the real Verizon employees' emotions to be exploited by times of scarcity and impair decision making as they feel empathy for the hacker. This is corroborated by Gragg (2003), who argues that people are more easily persuaded to do something questionable when there is pressure, surprise, or overloading.

This allowed the hacker to retrieve personal details from Brennan's account which were used to hack into his AOL email. Screen shots of the documents were then published on twitter accounts, allowing the members of the CWA to post documents in confidence and enabling them to humiliate their target without a sense of personal responsibility. This is just one example of why it will be useful for companies to raise their awareness of cyber criminals behaviours that may lead to hacks and security breaches.

SMART HOMES

by Jaime

Hands up who has an Alexa, a smart TV, a smart fridge, a semi-autonomous vehicle, an intelligent hoover, a smart oven, or a baby monitor at home. Numerous research journals claim the biggest challenges of smart home networks and devices as authenticity, privacy, integrity along with the limits these devices currently have regarding hardware resources.

Nowadays smart devices do not allow robust data processing, strong encryption mechanisms protecting the privacy of the data, or secure authentication mechanisms to validate and provide access to legitimate users. A hacker getting unauthorized access to personal information via our home devices could lead to giving away information that could be used for social engineering purposes to create extortion, or steal card payment details for instance. If users hold personal health devices, it could get eavesdropped or tampered, so the doctor assigns the wrong medication to the patient.

As a Cyber Security Analyst, I do not want to imagine what could happen if my personal information falls into the wrong hands. Unauthorized actions on the internet are getting sophisticated as hackers are getting smarter as well. Cyber researchers were able to develop a feature for Alexa Echo Dot to record personal conversations without the consent of users. A hacking group named “Orangeworm” were performing since 2015, installing viruses and getting unauthorized access to compromised computers stealing sensitive data and entering to medical devices connected to the network such as X-Ray and MRI machines.

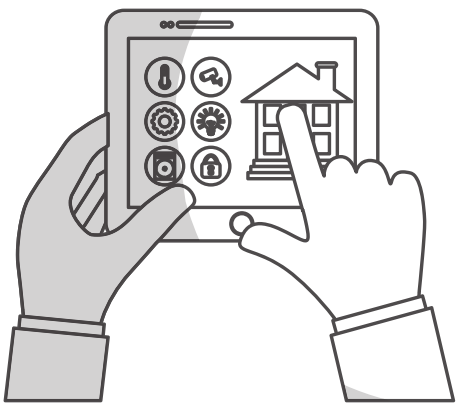
The question arises naturally, is my stored data disclosed to authorized users as the provider proposes? Or whether my data is being used for the only claimed purposes?

The journal from Mendelson (2017), proposes a regulatory framework to protect personal information. However, this is focused within the use of big data environments, which mentions the following: “In respect of governance, one of the most important drawbacks is either over-regulation or insufficient regulation”. Based on this framework, The CyberFish is proposing training sessions for everyone to stay aware and protect their personal data and their family members as well.

It is important for people to understand the fact that, the new European Global Data Protection Regulation (GDPR) is created with the main purpose of creating a culture of awareness in order to achieve personal data assurance. In fact, organisations must receive the corresponding consent from users for the creation, manipulation or deletion of data. However, people are accustomed to accepting terms and conditions from any application or device without even knowing the likely risks under the usage of them.

The responsibility of being safe on the internet now belongs to everyone. The more devices we connect to the internet, the more risks our data is being exposed. Regardless of an office or home environment, people must get constantly updated and trained immediately to avoid unauthorized data theft.

With a view to protecting home networks, our new series of workshops help individuals understand the exposure and the top tips to mitigate the risks regarding personal information leakage. The most effective method for stealing data is throughout social engineering. However, we offer people training sessions regarding basic cybersecurity measures to lower these risks and tackle social engineering threats.



WIFI RULES

by John

John joins our Executive Advisory Board in May. He will be helping us with special projects. This is his first infographics that helps navigate wifi connections when out and about.

Get in touch to get a copy of all our educational resources free to use in your awareness training, discuss over a family dinner or discuss with your parents.

Our free resources include:

- How to Rule Your Passwords
- How Cyber Criminals Chose their Victims
- Social Media Do's and Dont's
- Cyber Hygiene 101
- Cyber Risks of Individuals on the Autism Spectrum

Let us know if you would like to hear about a specific subject on hello@thecyberfish.com

WIFI SAVVY
with The CyberFish

Desperate to get connected while on the move? Need to reply an urgent email before getting on the next flight?
Before you say 'Horray' after you found a free public wifi, think about how to protect yourself from a potential cyber attack.
Here are our tips.

Always use public wifi with caution and assume it is vulnerable. Just because the wifi is provided by a big brand chain cafe or 5-star hotel does not mean you are automatically protected.

Never access sensitive personal data like banking / account details. Do not shop online, or change your password, or any login credentials when using a free and public wi-fi connection.

Turn off automatic wifi and bluetooth connections if your devices are not in active use (e.g. in your handbag and pocket), otherwise they can connect to a network without you even knowing it.

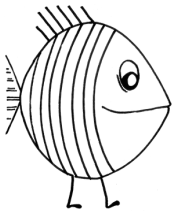
If you can, use 3 or 4G and switch on your personal hotspot. Connect to your own network to check sensitive information when out and about.

Beware of a rouge WiFi access point (sometimes called evil twin) created by a hacker using a nearby legitimate (the good twin) WiFi access point. Usually the signal of evil twin is strong so devices will rank it automatically up at the top of the perking order. Innocent users may usually select the one at the top, especially if the evil twin doesn't need a password to access. The user may think 'oh yeah i got a free wifi', the hacker essentially has access to all data flowing through the evil twin.

To avoid this, always ask e.g. coffee shop employee, concierge etc. to obtain the precise name of the public wifi. Alternatively, try to find a public wifi that at least requires some kind of login procedure.

THE CYBERFISH
Smarter on-line.
www.thecyberfish.com

CYBER GIRLS FIRST



WATCH THIS SPACE...

The CyberFish is branching beyond girls in STEM with CyberGirls First!

By focusing so heavily on helping scientifically-minded young women to get into STEM careers (including cybersecurity), are we neglecting the needs of those girls of a more artistic persuasion? This is an important question. After all, you don't have to be an engineer to rise to the C-suite.

And cybercrime will be just as relevant to these girls when they get there (and on their way up), no matter what they studied.

Hosted by Fieldfisher and backed by GCHQ&NCSC we are organising a series of events for Newham and Tower Hamlets schools starting in September, talking with girls about cyber security careers: technical and non-technical alike!

We are looking to discuss the role of ongoing and engaging education in communicating to this often overlooked group – equipping them to not only protect themselves but to thrive in a digital world, and bring the businesses of the future with them.

Save the Dates...

CYBER SECURITY CAREER PATHS

The cybersecurity skills gap is a hot topic of conversation at the moment. We help people find their way to the cyber security industry.

DIGITAL RISK STRATEGY WARGAME

Register your interest to participate in our tabletop simulation exercise today.

Booking is required for all our events via thecyberfish.eventbrite.com

SMART HOMES SECURITY

Learn more about how to keep your home networks to yourself by signing up to a free event on Smart Homes Security in June and July.