EMPLOYEES GUIDE

CYBER SECURITY TIPS

V1.3 FEB 2019

Introduction

CYBER SECURITY TIPS FOR EMPLOYEES

According to the National Crime Agency - In proportion to the total number of crimes, cyber-crime now accounts for more than 50% of all crimes in the UK. And the rate of cyber crime continues to increase. Think about it for a moment, criminals can now make money from the comfort of an arm-chair with little risk of being caught in comparison to traditional crime such as stealing physical items.

When developing cyber-security programs, many businesses focus on protecting their infrastructure perimeter and device endpoints. After all, that's traditionally where cyber-criminals usually first gain access and wreak havoc. However intelligent criminals no longer target devices - they target people as this is the easiest point of compromise in a companies security defence. Known as social engineering, hackers can now profile and target businesses at there weakest point. And the shocking reality is it's much easier than you might think.

Cyber security isn't a point in time exercise its an ongoing and evolving effort. Adopt best practices and create a stable foundation in your business. This document outlines some of the key tips your employees can use today.

CHAPTER ONE

PHYSICAL SECURITY

Keep a clean desk (yes really)

It makes complete sense and sounds so simple, but keeping a clean desk is often overlooked when talking about data security. It's also the perfect place to start the discussion with employees. Employees that keep a cluttered desk tend to leave USB drives and smartphones out in the open. They also often forget to physically secure their desktops and laptops so someone can't simply walk off with them. A messy desk also makes it more difficult to realise something is missing such as a folder with hard copy print-outs of customer lists. In addition to increasing the likelihood of something being removed, a cluttered desk means that the discovery of any theft will likely be delayed—perhaps by days or even weeks if the employee is out of the office. Such delays make it more difficult to determine who the perpetrator is and where the stolen material might now be located. Encouraging employees to maintain a neat desk pays off in two ways. In addition to making digital and paper assets more secure.

Common Mistakes to Avoid

The following list presents 11 "messy desk" mistakes employees make which could cause irreparable harm to the business, the employee, fellow employees, customers and business partners. These are all bad habits for which to educate employees to stop:

- Leaving computers unlocked.
- Placing documents on the desk that could contain sensitive information.
- Forgetting to shred documents before they go into the trash or recycling bin.
- Failing to close/lock filing cabinets
- Leaving mobile phones and USB drives out in the open.
- Neglecting to erase notes on whiteboards.
- Leaving bags out in the open
- Writing user names and passwords on slips of paper or post-its
- Leaving behind a key to a locked drawer
- Displaying calendars in the open or on the screen for all to see
- Leaving wallets and credit cards out on the desk

CHAPTER TWO

EMAIL THREATS

Social Engineering Inboxes and VoiceMail

Social engineering is non-technical, malicious activity that exploits human interactions to obtain information about internal processes, configuration and technical security policies in order to gain access to secure devices and networks. Such attacks are typically carried out when cyber-criminals pose as credible, trusted authorities to convince their targets to grant access to sensitive data and high-security locations or networks. An example of social engineering is a phone call or email where an employee receives a message that their computer is sending bad traffic to the Internet. To fix this issue, end users are asked to call or email a tech support hotline and prompted to give information that could very likely give the cyber-criminal access to the company's network.

Phishing Email Compromises

One of the most common forms of social engineering is email phishing - an attempt to acquire sensitive information such as usernames, passwords and credit card data by masquerading as a trustworthy entity. Phishing is likely the #1 primary email threat employees need to focus on. Such emails often spoof the company CEO, a customer or a business partner and do so in a sophisticated, subtle way so that the victim thinks they are responding to a legitimate request. Among the reasons these scams succeed are the appearance of authority—staffers are used to carrying out CEO instructions quickly. That's why phishing can be so easy to fall victim to.

Did You KNOW?

An attacker resides within a network for an average 146 days before detection!

Source: Microsoft

Four Common Phishing Techniques

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these four tactics:

- Embedding links into emails that redirect users to an unsecured website requesting sensitive information.
- Installing Trojans via a malicious email attachment or posing ads on a website that allow intruders to exploit loopholes and obtain sensitive information.
- Spoofing the sender address in an email to appear as a reputable source and requesting sensitive information.
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Email Security Best Practices: Five Ways to Block Phishing Attacks

Employees should always be suspicious of potential phishing attacks, especially if they don't know the sender. Here are five best practices to help employees avoid being victims:

1. Don't reveal personal or financial information in an email - Make sure employees also know not to respond to email solicitations for this information. This includes clicking on links sent in such emails.

2. Check the security of websites - This is a key precaution to take before sending sensitive information over the Internet. Check the page is using a valid security certificate. Also consider if employees are practising safe browsing habits. Sites that do not serve a legitimate business purpose are also more likely to contain harmful links.

3. Pay attention to website URLs—Not all emails or email links seem like phishing attacks, so employees may be lured into a false sense of security.

4. Verify suspicious email requests - Contact the company they're believed to be from directly. If an employee receives an email that looks odd from a well-known company, instruct them to contact the company directly - don't hit reply.

5. Keep a clean machine - Using the latest operating system, software and Web browser as well as antivirus and malware protection are the best defences against viruses, malware and other online threats.

CHAPTER THREE

USERNAME & PASSWORD MANAGEMENT

Low Security Account Credentials

Although it should be common sense, employees need to avoid the use of passwords that are easy for hackers to guess. Among the top ten worst passwords according to www.splashdata.com are those that use a series of numbers in numerical order, such as <123456>. The names of popular sports such as and are also on the list as are quirky passwords such as and even the word itself.

Six Tips to Strengthen Password Security

1. Change passwords at least every three months for non-administrative users and 45-60 days for admin accounts.
2. Use different passwords for each login credential.
3. Pick challenging passwords that include a combination of letters (upper and lower case), numbers and special characters at least 12 or more characters.
4. Avoid personal information such as birth dates, pet names and sports.
5. Keep personal (Social Media, Shopping etc.) passwords different from work ones.
6. Use two factor authentication wherever possible.

CHAPTER FOUR

MOBILE SECURITY

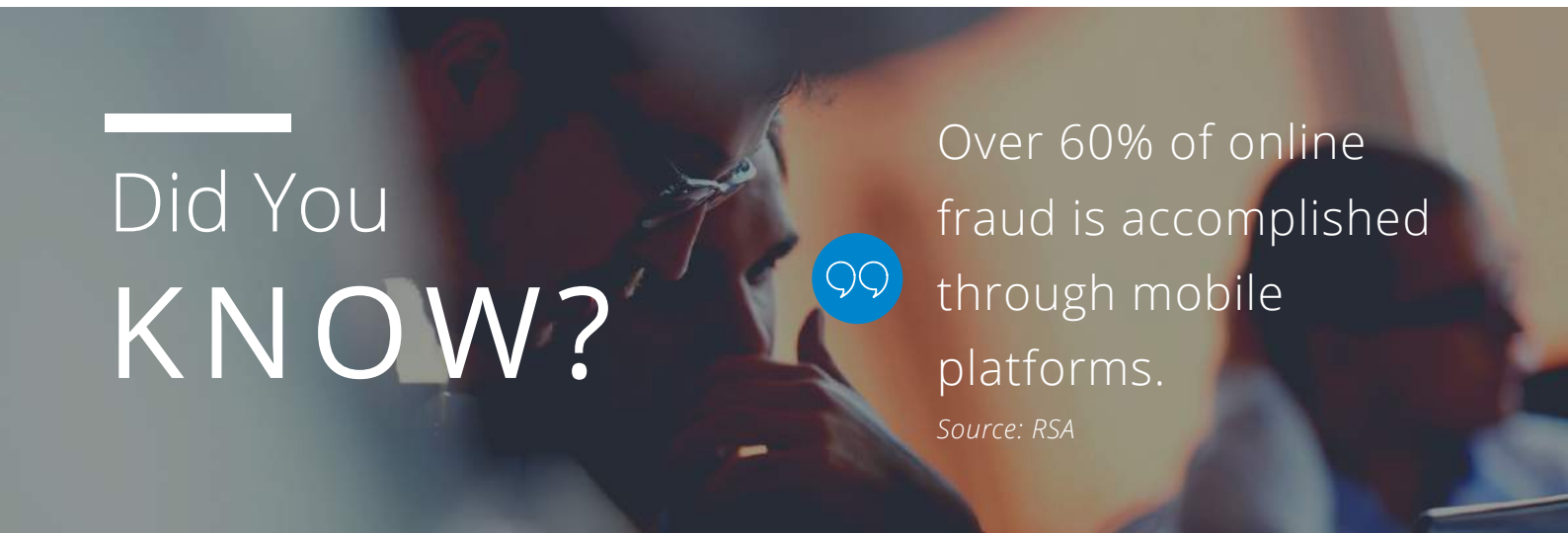
Mobile Threats Jeopardising Company Data

Mobile security is increasingly becoming a big concern as more and more companies adopt Bring Your Own Device (BYOD) environments, which allow end users to connect to corporate networks through their own (often multiple) devices. Even in cases where a business does not offer BYOD, end users often find a way to log onto business networks on their own.

With personal devices accessing corporate networks, businesses must now protect endpoint devices - that are not completely under their control, which opens up the business to greater risk. Trying to gain control over personal devices also presents the challenge of making sure the company does not infringe on personal apps and information employees store on their own devices.

Mobile Device Security Challenges

- Lost, misplaced or stolen devices—remote wiping them quickly is key to protecting sensitive business and personal information.
- Mobile malware—hackers are now turning their attention to mobile devices and executing successful breaches through text messages to both iOS and Android devices.
- Unsecure third-party apps - if breached, can serve as a gateway to other apps on a device and the device operating system, where security controls can be manipulated.
- Using Public and Guest WiFi HotSpots without appropriate protection means hackers can hijack devices or steal data/information in transit.



CHAPTER FIVE

SECURE WEB BROWSING

Top Browser Threats

When end users venture out onto the Internet, it's easy to get tangled up in the vast web of threats lurking on many website pages. Some of them are readily apparent, but others are well hidden. Malvertising - a form of malicious code that distributes malware through online advertising—can be hidden within an ad, embedded on a website page, or bundled with software downloads. This type of threat can be displayed on any website, even those considered the most trustworthy.

End users also need to beware of social media scams. Hackers have created a playground of virtual obstacles across all the major social media sites such as Facebook and Twitter, using malicious links, fake pages and other methods.

Web Browsing Best Practices

- Be conservative with online downloads.
- Beware of antivirus scams.
- Interact only with well-known, reputable websites.
- Confirm each site is the genuine site and not a fraudulent site using protection.
- Determine if the site utilises SSL (Secure Sockets Layer), a security technology for establishing encrypted links between Web servers and browsers.
- Don't click links in emails - go to sites directly.
- Use social media best practices.
- Keep browsers up-to date
- Be careful of browser plugins, even if downloading from the browser store

CHAPTER SIX

TRAINING

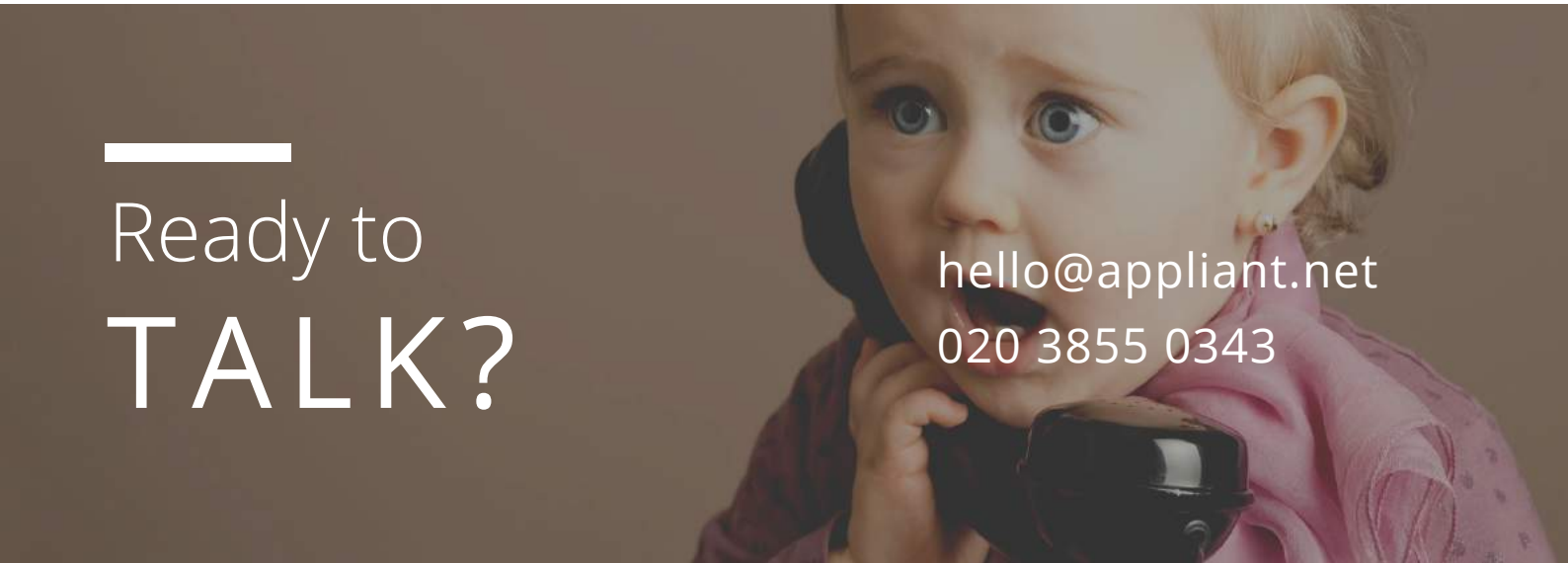
The Human Firewall

Modern cyber threats target individuals not devices, known as social engineering the biggest weakness in any organisation is it's people. Whether being tricked into a false sense of security and letting a stranger into the building or being profiled online and targeted. We are all vulnerable and the all the best cyber security in world can't prevent human error. The human firewall is often the first and last defence in your cyber security chain.

Taking the time and effort to train yourself and your team in best practices will not only protect you in the workplace but also help protect yourself at home from cyber threats.,

Education and Technology: A Winning Cybersecurity Combination

As your business begins the journey to enhance its cybersecurity posture, it all starts with educating your employees. The tips provided within this eBook along with some basic common sense can go a long way in making sure sensitive information does not fall into the wrong hands. proactively identify and thwart potential attacks as well as react expediently if a successful attack occurs. This is where a managed IT services provider can assist. They eliminate the need for your business to keep up on the latest antivirus, antimalware and alert technologies.



www.appliant.net

020 3855 0343