Loss prevention standards

Cyber Security:

Top 12 Tips to Protect Against a Cyber Attack

The global COVID-19 pandemic has led to a significant increase in cyber attacks as criminals target vulnerable people and systems. This document provides information on how to protect against a cyber attack.

Cyber Security:
Top 12 Tips to Protect Against a Cyber Attack

Introduction

Cyber attacks and infiltrations, aimed at all sizes of business and at individuals, have increased dramatically. Cyber criminals now attempt to use any topical subject, including the COVID-19 pandemic, to prey on people and systems, whilst they are at their weakest.

The Business Continuity Institute publish their Horizon Scan Report annually: BCI Horizon Scan Report 2020. This report has been an excellent indicator as to what businesses have seen as the biggest impacts on their organisation in the previous 12-months, and what their biggest concerns are for the coming year. Historically cyber attacks were a minor issue, but over the last few years have become a large, real impact across all sectors, and one of the biggest fears for businesses in the coming years. The 2020 report shows cyber attack and data breach as the threat with the greatest likelihood to happen, and the greatest likely impact, clearly showing the concern businesses have.

Aviva Risk Management Solutions have looked at cyber crime reported to the Police via Action Fraud, and to the National Cyber Security Centre, to put together 12 areas that businesses would need to consider when looking at solid protections against cyber intrusions, and the lasting impact they can have on activity, income and reputation.

Real-Life Examples of Cyber Crime

Date: 19 June 2020
Headline: '*Over £16 million lost to online shopping fraud during lockdown, with people aged 18-26 most at risk'**

Despite retail and non-essential shops re-opening across the UK, many of us continue to shop online. Action Fraud, the UK's national reporting centre for fraud and cyber crime, is warning the public to remain vigilant and take extra care online after statistics show 16,352 people fell victim to online shopping and auction fraud in the lockdown period imposed during the COVID-19 pandemic.

Since shops were forced to close due to the coronavirus outbreak on 23 March, Action Fraud has received reports of online shopping fraud totalling £16.6million in losses.

Advice is to be more aware of who you are in contact with regarding the purchase, research the seller and feedback from other customers and make checks into whether an advert could be a phishing attempt.

*Reference: Action Fraud – National Fraud & Cyber Crime Reporting Centre

Date: 27 May 2020
Headline: *'260 reports of coronavirus-related TV Licensing emails so far this month'***

The emails purporting to be from TV Licensing claim that the recipient's direct debit has failed and that they need to pay to avoid prosecution. Recipients are told that they are eligible for a 'COVID-19 Personalized Offer' of six months free. The messages contain links to genuine-looking websites that are designed to steal personal and financial information.

Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text.

**Reference: Action Fraud – National Fraud & Cyber Crime Reporting Centre

There have been numerous others, with very realistic fake emails looking like they were from the National Health Service (NHS), UK Government, World Health Organisation, Tesco, and Amazon among others.

Cyber Security – Top 12 Tips

1. Password Complexity and Management

It is essential for businesses to protect their information and data stored, by ensuring users access systems by entering a strong password. A system needs to be in place to make sure rules are complied with. Using capitals, lower case letters, numbers and special characters over a minimum number of digits, usually eight (the more the better) is a good rule, for example, £Magenta6. The National Cyber Security Centre recommends using three random words, for example, bluemonkeyflag, and this could be made more complex and secure by adding numbers and special characters, e.g. 27bluemonkeyflag&.

There are certain words/details that should never be used, such as date, place of birth, favourite football team, pet's name, partner or children's name, etc. These can be found by cyber criminals or could be relatively easy to guess.

2. Multi-factor Authentication (MFA)

Having two forms of identification to gain access is a simple and effective way to increase your information/data security. This can be achieved by password and then a randomly generated code, sent to you by text message or an app. There are a number of possible ways to provide MFA, and this will greatly increase security.

3. User Privileges

A rule that should always be applied, but especially important where employees are working remotely. In short, give individuals access only to those systems, functions, software and areas that they need to do their job. Allowing blanket access can provide employees or contractors with access to secure areas of the business that they may not even realise they have. Should they gain access into a user account, this leaves the system open to cyber criminals.

4. Virtual Private Networks (VPN)

A VPN extends a private network across a public network, allowing users to send and receive data as if their devices were connected to the private network. This will give the data the benefit of the private network's security including password protection, and encryption.

5. Use of Own Equipment

Allowing your users to access your business' network from their own devices can introduce security issues. Any device supplied by the business should be a standard build with security and restrictions in place to protect the business' data and information. A user's own laptop for example, could already be infected and introduce a virus into the network. Even if it is not infected it could well have out of date security or anti-virus software.

There can be the issue of individuals sharing use of the device with family members, increasing the potential for accidental data loss. It could also be that data loss, or an infiltration, goes on longer without detection due to the lack of monitoring, etc.

6. Phishing

Phishing is defined as untargeted, mass emails sent to many people asking for sensitive information such as bank details, or encouraging them to click on a link, or visit a fake website. Training employees to recognise a phishing email is essential as they can be very convincing.

Some points to remember include:

- Look at the email address it has come from. If it is supposed to be from Amazon, for example, does the email address look correct?
- Look at the grammar and spelling. If the email is supposed to be from a big business, retailer, etc., they would be far less likely to make such mistakes. A lot of phishing attempts originate outside the UK and spelling, etc. can be a giveaway
- Is it addressed to you by name? If it is simply to Dear Customer, this can be a sign the sender does not know you, or deal with you
- Threats requesting payment. Send details 'within 24 hours', etc., is not a usual business practice
- Is it too good to be true? A phishing attempt saying you've won a dream holiday needs looking into in more detail, you would more than likely remember entering. Check sender address or search the internet for details

There are two other terms it is useful to know, for a more specific, targeted, attack:

Spear-phishing: This is a targeted form of phishing. The email is designed to look like it's from a person the recipient knows and/or trusts

Whaling: Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives

7. Removable Media

Use of unsolicited removable media, such as SD cards or USB memory sticks, can introduce viruses into a computer, which can spread through a network. There should be a policy that no removable media is to be used, and the ports on devices disabled to protect against this threat. Where memory sticks have previously been used internally in the business, use email or cloud storage to transfer the data instead.

8. Public Places

There are three main things to keep in mind when using devices in public:

- Security: All users should be trained on the exposure when leaving devices unattended in public. Even if using washroom facilities; phone, tablet, laptop, etc. should be taken with you
- Data: Users should be aware of who and what's around them. Can someone look over your shoulder, etc.? They not only could see what's on your screen, but may see keystrokes, etc. that give away passwords
- Wi-fi: An unsecure wi-fi network is an exposure. Wi-fi in a coffee shop for example, with no password, could provide easy access for cyber criminals. These unsecure networks should not be used at all. Even if a password is required in such circumstances, it may be available to all, insecurely displayed on a wall, it might not have changed for months and may be seen from outside the premises. If an individual must use a wi-fi hotspot, a mobile phone's own 4G network has inbuilt security and tethering that improves the security

9. Encryption

This is the process of encoding a message or information in such a way that only authorised parties can access it. It will not on its own, stop an attack, but it does make the data useless to the cyber criminal.

This is a very good security measure and should be considered to protect all data being transferred.

10. Reporting Security Issues

Employees and contractors with access to your systems should be made aware that the time taken to report any security incident is absolutely critical. Whether it's a lost phone, a stolen laptop, any breach of systems or network, opening or clicking on a suspicious email attachment or a link, a password you think may be compromised, use of an unapproved removable media device or any other threat or activity that causes a user concern, all must be reported as soon as possible. Being able to assess the situation quickly and organise a suitable response could help maintain a level of security, limit losses, speed up recovery and also increase the chances of a perpetrator being caught.

11. Anti-virus and Software Updates

Software updates include the latest security enhancements and patches for an application. So, while software updates can sometimes be an irritation to users, e.g. they can take too much time to download, it cannot be emphasised strongly enough that as soon as an update is available, it should be completed. This point should be made clear to all employees and contractors.

12. Quick Reference Guides

If, for whatever reason, your business has a large number of remote workers, e.g. as a result of an incident closing a location or a pandemic outbreak, then uncertainty about accessing the network remotely, or unfamiliarity with different systems and applications, can give rise to an increased demand on your IT Helpdesk. Depending on the issue, this team could in itself have reduced employee numbers, or the number of remote workers to IT Helpdesk team members ratio increases, so placing increased burdens on the resource available. Therefore, production of easy to use, brief and accurate 'How To' user guides can reduce the impact on the IT Team, and also reduce the chance of employees creating a security issue.

Definitions

Virus

A virus is piece of software that can replicate itself and spread from one computer to another.

Antivirus

Software designed to detect, stop and remove viruses and other kinds of malicious software.

Trojan

A type of malware (malicious software) or virus designed as legitimate software, that is used to hack into the victim's computer.

Ransomware

Malicious software that makes data or systems unusable until the victim makes a payment.

Social Engineering

Manipulating people into carrying out specific actions or divulging information, that's of use to an attacker.

Water-holing

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Firewall

Software that uses a defined rule set to constrain network traffic, preventing unauthorised access to a network.

Social Engineering

Manipulating individuals into carrying out specific actions, or divulging information of use to an attacker.

Key-logger

Tracks the keys struck on a keyboard, typically in a covert manner, so the keyboard user is unaware.

Penetration Testing

A method of evaluating the computer security of a system or network, by simulating an attack, from malicious persons, inside or outside an organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- The National Cyber Security Centre
- Action Fraud

Additional Information

Relevant Aviva Loss Prevention Standards

- Pandemic Planning & Coronavirus
- Pandemic Recovery: 'New Normal' and the Post-Pandemic Business World
- Cyber Security, Homeworking and the Coronavirus

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 03453666666*

*Calls may be recorded and/or monitored for our joint protection.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

13/08/20 V1.1

LOSS PREVENTION STANDARDS