COVID -19 - Cyber Security

Loss Prevention Standard

Cyber Security, Homeworking and Coronavirus

Introduction

In Ireland, and around the globe, businesses and individuals are doing their best to cope with the Covid-19 pandemic. With normal daily lives and normal business practices under pressure, due to measures to slow down the spread of the virus, it has meant changing how we do things. This unfortunately has given cyber criminals an opportunity to take advantage of the situation, and a dramatic rise in cyber-crime has been noticed.

Organisations are in a position where they need to have more remote workers. Cyber security experts have seen that attackers move quickly to launch phishing attacks around other threats or humanitarian disaster events, and Covid-19 has given them an opportunity to attack work and personal computers as well as home networks.

The current situation has seen unprecedented moves by all types and sizes of business, in a very short space of time, to enable the vast majority of their staff to work from home. This has put a considerable stress on infrastructure and support systems.

12 Recommendations for cyber security when remote working are:

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 recommend 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. 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.

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.

User Privileges

A rule that should be applied at all times, but is especially important where staff are working remotely. In short, just give individuals access to systems, functions, software and areas, that they need to do their job. Allowing blanket access can provide members of staff with access to secure areas of the business that they may not even realise they have, leaving this open to cyber criminals, should they gain access into a user account.

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.

Use of Own Equipment

Allowing your users to access your businesses' 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 businesses' 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.

Anti-virus and Software Updates

Sometimes software updates can be an irritation to users, as they can take time, but 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 staff, as the latest updates will also include the latest security improvements.

Quick Reference Guides

If your business has a large number of remote workers as a result of an incident closing a location, or a pandemic outbreak, knowing how to access the network remotely, and use of systems and applications that can be quite different to the usual procedures, can give rise to increased query traffic to your IT Helpdesk, which itself could have reduced manning. Production of easy to use, brief and accurate 'How To' user guides can reduce the impact on the IT Team, but also reduce the chance of staff creating a security issue.

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 staff to recognise a phishing email is essential as they can be very convincing, but there are some points to remember:

- 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 very unlikely to make 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, that 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/google the details

Cyber criminals are preying on the fears connected with the coronavirus. Selling a cure or providing a map of affected areas are phishing attempts already seen by the National Cyber Security Centre. Staff need to be vigilant, only use the HSE or World Health Organisation websites for accurate details of the situation, and take care not to click on links sent in emails, etc.

Removable Media

Unsolicited 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.

Public Places

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

Security: All users should be trained to never leave devices unattended in public. Even if using washroom facilities; phone, tablet, laptop should be taken with you.

Data: Users should be aware of 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: Wi-fi in a coffee shop for example, with no password, has easy access for cyber criminals. These should not be used at all. Even if a password is required it may be displayed on a wall, may not have changed for months and may be seen from outside. If a user must use a wi-fi hotspot, a mobile phone's 4G network has inbuilt security and tethering that improves the security.

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.

Reporting Security Issues

Staff should be made aware that time is of the essence when it comes to reporting any security incident; whether it's a lost phone, stolen laptop, any breach of systems or network, clicking on a bad email attachment or a link that doesn't look right, a password you think may be compromised, or any other threat or activity that causes a user concern. 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.

Definitions

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

Phishing
Defined as untargeted mass emails attempting to get a person to provide sensitive information.
Within this there are two other terms:
- **Spear-phishing:** 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.

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.

Sources and Useful Links

The National Cyber Security Centre – Home-working: preparing your organisation and staff

Additional Information

Relevant Aviva Loss Prevention Standards

Pandemic Planning and the Coronavirus

Further risk management information can be obtained from Aviva Risk Management

Please Note
This document contains general information and guidance and is not and should not be relied on as specific advice. 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. Aviva accepts no responsibility or liability towards any person who may rely upon this document.

AVIVA

| Retirement | Investments | **Insurance** |

B244.03.20