Loss prevention standards

Cyber Security:

Top 12 Tips to Protect Against Cyber Attacks

Version: 1.2
Date: 20th December 2023

This document outlines 12 key recommendations that individuals and organisations should implement to help safeguard their systems and data from cyber security attacks.

AVIVA

Cyber Security: Top 12 Tips to Protect Against Cyber Attacks

Introduction

As the use of technology grows rapidly in our businesses, and our personal lives, so do the threats to technology from criminals via hackers working for hostile countries, and the spread of false information. In 2023, we saw attacks on power plants, technology companies with billions lost in crypto scams, and numerous related cyberattacks related to Russia's war with Ukraine.

Attacks such as morphing ransomware variants (ransomware attacks that continue to evolve into new forms that take advantage of vulnerabilities), software and hardware supply chain exploitation, increased cloud infrastructure attacks, cryptocurrency volatility, cybercrime, IoT (Internet of Things) and operational technology breaches are on the rise, yet many people and organisations still do not have measures in place to protect against these attacks.

Even though these cybersecurity challenges seem complicated, regular internet users and organisations face the risks of major breaches. For example, common password leaks and simple account hacks can lead to identity theft of employees. The information gathered can be used to wipe out an entire organisation's database. While it is difficult to prevent sophisticated attacks, for example from nation-states and other cyber threats, taking simple precautions like multifactor authentication can block most malicious attempts. Organisations must continuously monitor their systems limit access.

Getting expert guidance on practical habits for browsing websites, using social media, and storing sensitive information is more vital than ever in today's world impacted by conflicts and geopolitical tensions. Governments working with technology companies can also help adopt safer systems like fingerprint or facial recognition login. However, outdated computer systems and less-trained cybersecurity professionals will continue to remain as a problem. This is unless more funding and training is focussed on resourcing and upskilling experts to be cyber threat ready and improving critical digital infrastructure. By learning about these risks, employees, companies, and governments can work together to reduce cyber threats through public awareness and employee trainings.

Aviva Risk Management Solutions have looked at Global Impact events, cybercrime reported to the Police via Action Fraud and to the National Cyber Security Centre, to put together twelve 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.

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 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 several ways to provide MFA, and this will 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:

- Look at the actual email address from the sender. If it is supposed to be from specific organisation, does the email address look correct and reflect that organisations name? Phishing attempts can originate from any country.
- Look at the grammar and spelling. If the email is supposed to be from a reputable business, retailer, etc., they would be far less likely to make spelling and grammar mistakes. Inappropriate or incorrect spelling, grammar and/or language use can be a sign that the email is not from a trusted source.
- 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 have won a dream holiday or a prize, needs investigating in more detail. In addition, you would more than likely remember entering such a competition. It is important to check the 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 is 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 of leaving devices unattended in public or insecure places. Even if using toilet facilities; phone, tablet, laptop, etc. should be taken with you.
- Data: Users should be aware of who and what is around them. Can someone look over your shoulder, etc.? They not only could see what is on your screen, but may see keystrokes, etc. that can give away passwords for example.
- 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.
    - May be visible 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 to 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 cybercriminal.

This is an exceptionally 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 critical. Whether it is 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 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 and reinforced as appropriate.

12. Quick Reference Guides

If, for whatever reason, your business has many remote workers, e.g., flexible or hybrid working; because of an incident closing a location or a global impact event such as 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 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 reduce the chance of employees creating a security issue.

Definitions

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

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

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.

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, which is of use to an attacker.

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

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

Water-holing: Setting up a fake website (or compromising a real one) to exploit visiting users.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.
For more information please visit:
Aviva Risk Management Solution-Specialist Partners

Sources and Useful Links

- National Cyber Security Centre (NCSC)
- ActionFraud

Additional Information

Relevant Loss Prevention Standards include:

- Business Impact Analysis
- Business Continuity Planning

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 0345 366 6666. *

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

Please Note

Version: 1.2
Date: 20th December 2023
Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.