Acronyms
Tailored IT and Unified Comms

Cyber Security & What Your Business Needs To Know

Contents

Cyber crime is the greatest threat to every profession, every industry, every company in the world.

Ginni Rometty
Chairwoman, President and CEO
IBM

The different types of cyber crime that threaten your business.

Spyware

Software that allows a third party, unbeknownst to yourself, to gain information about the activity on your computer.

Phishing

An attempt to gain sensitive information from you by directly asking for it, often whilst posing as a well known, legitimate company.

Ransomware

Software that allows a third party, unbeknownst to yourself, to gain information about the activity on your computer.

Cryptojacking

The unauthorized use of an individual's or company's processing power to mine cryptocurrency such as Bitcoin.

Denial of Service Attacks

Multiple requests that flood a system or network, starving it of bandwidth and freezing it, making it impossible to use.

Bruteforce Attacks

An attempt to log into someone else's system or accounts by trying many multiple passwords consecutively, very quickly and often.

Security advice that you can share within your business to minimise the risk of cyber crime.

Use strong passwords.

Use a mix of letters, numbers and symbols and don't use the same password for multiple sites. Don't share your password and don't write it on a post-it note attached to your monitor.

Think before you click.

Always be careful when clicking on links or attachments within emails. If you're suspicious for any reason - don't click it! Just because someone says they're apple, it doesn't mean they are.

Backup, backup, backup!

Backing up your machine and data regularly can protect you from the unexpected. Make sure you know how to retrieve a back up too, should you need it.

Remain conscientious.

Be wary of what you plug into your computer. Malicious software can spread via infected flash drives and smartphones.

Use protective software.

A number of cyber attacks can be prevented by using up to date anti virus software and spam software. Used in conjunction with firewalls, you can fend off a number of threats.

Security advice that you can share within your business to minimise the risk of cyber crime.

Browse carefully.

Banking or shopping should only be done on a device that belongs to you, or on a network that you trust. Install bank security software and ensure your browser is blocking pop ups.

Patch, patch, patch!

Patches and updates are released to ensure a product is equipped to fight the latest security risks. Not updating your software or hardware leaves you and your entire network vulnerable.

Involve everyone.

Ensure that all of your employees know how to spot a threat and they are kept up to date best practices. They are your first line of defence.

It's estimated that the cumulative global spending on cyber security products and services between 2017 and 2021 will exceed $1 trillion.

Cybersecurity Venutres

Security advice that you can share within your business to minimise the risk of cyber crime.

Calculate your down time.

If your network went down how many hours would it take you to fix it? If you don't know use a number of different hours to see potential costs and seek help clarifying this time span.

Calculate your losses.

If you couldn't work, because you couldn't use technology, how much money would you lose per hour? Include wages for non-working staff, loss of earnings and potential new hardware.

Multiply the two.

Multiply the number of hours you'd be down and your losses. If you don't know how long you'd take to recover, you can try a number of different time spans. The quicker you can react the better.

Seek professional help.

You can't control your losses in the event of a cyber attack. You can control your down time. Speak with a professional to minimise this time.

Acronyms

Tailored IT and Unified Comms

Find out more about Acronyms at www.acronyms-it.co.uk

@AcronymsLtd