Business Emergency Resilience Group
Preparing for cyber attacks and online fraud

What are the risks to my business?

Cyber attacks

Cyber attacks are deliberate exploitations of computer systems, information technology, and online emails impersonating genuine companies that you or your business may deal with. They can result in consequences that can compromise data and lead to cybercrimes, such as identity theft.

"A third of small businesses suffered a cyber-attack from someone outside their business last year. The average cost of a major security breach is between £65,000 and £115,000 and can result in a business being put out of action for up to 10 days." *[Telegraph, 24 Feb 15]*

Online Fraud

Online fraud is the use of the internet or software with internet access to gain a dishonest advantage, which is often financial, over another person, e.g. fraudulent purchase transaction or identity theft.

Phishing

- Emails impersonating genuine companies that you or your business may deal with.
- Often sent randomly to many thousands of people.
- Purpose is to trick the recipient into disclosing sensitive information, to direct them to a fake but genuine looking website or to download malicious software (malware) to their PC or device.

Trojans and viruses

- Trojans and viruses are sophisticated forms of malware which can be installed on your computer without you realising.
- Typically delivered via a phishing email or compromised website.
- Trojan and viruses can monitor your activity and corrupt your attempts to visit genuine websites by re-directing you to fake but genuine looking versions instead.

Spyware

- Spyware is malware that secretly eavesdrops on infected machines and reports everything back to the fraudster.
- A keystroke logger will record all of the keys you have entered onto your keyboard, allowing the fraudster to capture private information and passwords.
- Spyware can get into your system through phishing emails and infected websites.
- If your computer is infected by malware, it can have devastating consequences.

How can I prepare my business?

Visit the Cyber Essentials website

Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves against cyber threats. It provides information on good basic cyber security practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats.

Protect your computer

Whatever you use the internet for it is vital that you take a few basic steps to ensure that your computer is protected against the latest threats. Just as you protect your house with locks on doors and maybe a burglar alarm, it is essential that you protect your computer by using up-to-date anti-virus software, doing regular scans of your computer to check for viruses, installing a personal firewall, as well as downloading the latest security updates for your web browser and operating system.

Three steps to protect your computer:

1. Install and learn how to use personal firewall.
2. Use anti-virus software and keep it up to date on a regular basis.
3. Download the latest security updates (or patches for your web browser and operating system.

Here is how each type of protection works:

- **Antivirus** – helps to stop threats by scanning your computer and looking for suspicious files.
- **Firewall** – hides your computer from attackers and helps to stop criminals getting data in and out of your computer.
- **Online Security Software** – locks down the connection between your computer and your online banking service. It ensures that you are on a genuine website and not diverted to a fraudulent site.

None of these tools alone can guarantee 100% protection all of the time but together they will considerably reduce the chances of your computer becoming infected and fraudsters capturing your sensitive information.

"Recent research shows that 59% of consumers are put off shopping with small firms online, and 82% would buy more if they could show they were protected from cybercrime"

[gov.uk, 22 October 14]

Online Banking

Attacks on internet banking are becoming increasingly sophisticated and criminals are finding new ways to bypass traditional defences, meaning your antivirus and firewall software alone may no longer safeguard your business from fraud.

To help protect you when you are banking online, most banks offer free online security software to complement your existing antivirus and firewall software.

Online security software protects your online banking session by:

1. Shielding your log-on credentials and passwords from prying eyes.
2. Protecting your information and personal details, even if your computer is infected with malware.
3. Safeguarding your identity

It is important to use this software alongside your existing antivirus and firewall software. Find out if your bank offers this and install this straight away. The software will detect and quarantine malware and offer an extra layer of security to your anti-virus and firewall.

If you use online business banking, ask your bank to assess how you use it. For example, if you only make domestic UK payments it would be prudent to disable the international payment

Applying caution

Other precautions you could introduce include:

- **Keep up to date on current scams.** The very first line of defence against scams is knowing what they are and what is prevalent in your area. Your bank will publish information on current fraud scams, what they are and how to protect yourself from them. Other places to go for similar information are your local Police force website, Trading Standards, Citizens Advice Bureau, Financial Fraud Action and Get Safe Online.
- **Apply caution to all unexpected or unsolicited emails** - even if they appear to originate from a trusted source.
- **Be careful about following links or clicking on attachments in emails** – even if they appear to relate to an innocent subject, as they may contain malware which will infect your computer or device.
- **When keying sensitive information on a website, ensure that it is secure** – denoted by the prefix 'https' and locked padlock or unbroken key symbol. You can check the authenticity of a secure website by double clicking on this symbol-
- **Keep your passwords safe and secure, and change them regularly.** Longer is stronger – choose passwords made up of a mix of letters, numbers and special characters. Remember, passwords don't need to be a word! Why not choose a combination of your favourite things? For example, your favourite band (Coldplay) and football team (Aston Villa) could become C0ldv1ll@. Or maybe the registration of your first car would be a safe choice?

Find out more

www.bitc.org.uk/berg

#BERGResilience

Business Emergency Resilience Group