# Common threats to your Business' Cybersecurity

*For businesses of any size (small, medium or large), the risk posed by poor cybersecurity policies could cost them considerably.*

In the event of a cybersecurity incident, the long-term costs and consequences of such an incident can range from months to years and include significant expenses that companies are unaware of or do not anticipate in their planning.

These costs can include lost data, business disruption, revenue losses from system downtime, notification costs, or even damage to a brand's reputation.

There are many simple and inexpensive measures businesses can use to improve their security and prevent these issues from occurring.

## Scam Messages/Phishing

Scams are a common way that cybercriminals target small businesses.

Their goal is to scam you or your staff into sending money or gift cards, clicking on malicious links or attachments or giving away sensitive information, such as passwords.

If you are a small business, you should be especially careful of phishing attacks. These scam messages often link to a fake website and encourage unwitting recipients to login, giving them access to account information like passwords and login details.

Phishing messages can be sent in many ways, including emails, SMS, social media, instant messaging platforms, or even phone calls.

They can feature official-looking logos and disclaimers and typically include a 'call to action' to trick people into sharing sensitive and personal information, such as passwords and banking details, and much more.

## Email attacks

A common email attack against small businesses is a business email compromise (BEC). Through this, criminals can impersonate business representatives by using compromised email accounts, or through other means (such as using a domain name that looks similar to a real business's one). The goal of these attacks is to scam victims into sending funds to a bank account operated by the scammer.

The best way to defend against email compromises is by training and raising awareness for your employees. Ensure your staff know always to be cautious of emails with including requests for payments, especially if urgent or overdue change of bank details an email address that doesn't look quite right, such as the domain name not exactly matching the supplier's company name.

## Malware (Malicious Software)

Malware is a blanket term for malicious software designed to cause harm, such as ransomware, viruses, spyware and trojans. Malware can steal or lock the files on your device steal your bank or credit card numbers steal your usernames and passwords take control of or spy on your computer.

Your device can be infected by malware in many ways, including:

- visiting websites that have been infected by malware
- downloading infected files or software from the internet
- opening infected email attachments.

While anti-virus or security software can help protect you from malware, no software is 100% effective. Staff must be vigilant with emails, websites, and fi le downloads and regularly update their devices to stay secure.

As a general starting point for small/medium businesses, we recommend the following:

- turn on multi-factor authentication to add an additional layer of security (starting with your most important accounts).
- use a password manager to create and store unique passwords or passphrases for each important account (such as banking, emails, etc.).
- limit the use of shared accounts and secure any that are used in your business.
- create a plan or procedure for backing up your business regularly.
- determine a plan for how cyber security awareness will be taught in your business.