SYNAQ

CHEAT SHEET

SECUREMAIL IN **SIX EASY STEPS**

Cybercriminals will exploit any weakness in your security structure. They aim to crack open your inbox using brute force attacks or carefully crafted deception in the form of phishing, but there are some basic steps you can take to protect your network. Avoid becoming a statistic by following these six golden rules.

☐ USE **STRONG PASSWORDS**

This is a fundamental rule and cannot be repeated enough: strong passwords are essential. They should incorporate letters, numbers and symbols and not just your name or the name of your business, or worst of all, something like *password123.*

Change your password frequently and keep it safe, and avoid using the same password for multiple accounts. Consider using a trusted password manager with two-factor authentication if you have trouble keeping track.

☐ BE CAREFUL OF **LINKS, FILES OR ATTACHMENTS**

If you don't know who sent it, and even if you think you do, it's best to avoid opening any attachments or links that you didn't expect to receive.

Even if the sender is a trusted contact, their account may have been compromised. In fact, it's best to avoid clicking on links in emails altogether and to rather manually enter the URL for the site in question into your browser.

☐ KEEP **PERSONAL INFORMATION** TO YOURSELF

A reputable organisation will never ask you to send personal information – especially passwords or any credit card information – over email.

Even when emailing someone you know and trust, it's best to omit personal or financial information in case a third party ever gains access to it.

☐ LOOK FOR CLUES, **LIKE BAD SPELLING**

Scrutinise emails from organisations such as banks or service providers that look legitimate at a glance, especially if they require something from you (keeping the above points in mind).

A big clue is poor attention to detail and unprofessional mistakes, such as spelling errors or poor grammar. It will also be highly unusual for such an email not to be personalised.

☐ CHECK **DOMAIN NAMES** AND **IP ADDRESSES**

Nearly all email providers offer information about the sender on the message header.

If you hover your mouse over the address, a window should pop up with details that match the stated name and address. You have cause to be suspicious if it doesn't reflect the proper name of the company that supposedly sent it.

☐ SECURE YOUR **PROCESSES**

Some phishing attacks are directed at specific employees in an organisation and are usually disguised as an important instruction from a senior executive. This method is known as "whaling". Finance department staff are usually targeted with requests for money transfers or notifications of altered payment details on an existing client.

Such emails often don't contain links or attachments and rely on recipients to complete the requested action, exploiting their willingness to obey authority. A company's staff must be made aware of this practice and encouraged to verify such requests through another channel (such as a phone call) before carrying them out.

Learn more about securing your inbox.

CONTACT US