

Cyber Security Awareness Month

Why should we all play our part?

95%

The percentage of data breaches involving human error

91%

The percentage of organisations that experience data loss due to email phishing

295

The average time taken to identify and contain a phishing related breach.

It's not all doom and gloom!

Every click counts. By staying alert and taking small steps, we all contribute to keeping our business and data safe.

Let's all play our part!

7 Tips for Staying Cyber Safe

1. Think before you click

Hover over a link to reveal the destination URL. If it looks different from what you expect, don't click on it.

2. Look Out for Phishing and Social Engineering

If you receive a suspicious email or call, don't open, click on it or respond. Instead, follow up with your IT security department.

3. Go beyond passwords

Use passphrases and consider a password manager for storing and generating complex passwords. This enhances security and helps with remembering long strings.

4. Install updates

Always install the latest updates for your operating system, browser, and any applications installed on your device.

5. Think before connecting

Be cautious when connecting to unfamiliar Wi-Fi networks. Using a VPN can protect your data by creating an encrypted, private connection.

6. Charge with caution

Don't plug your mobile devices into any outlet you find. You could risk becoming the victim of malware or data theft.

7. Use multi-factor authentication

Using 2FA can add another layer of protection on devices or accounts where sensitive data is handled.

Let's all play our part!



Password Security Tips

Quick tips to help you safeguard sensitive information

Don't



Don't use
personal info

Avoid public Wifi

Never reuse
passwords

Never share
your password

Do



Randomise patterns
and sequences

Use a variety of
numbers, letters
and characters

Download a
password Manager

Prioritise password
length

Check your
password strength

Change passwords
periodically





Keep an eye out for these common phishing warning signs.

Sense of urgency

Illegitimate or unfamiliar address

Spelling and grammar mistakes

Generic greeting

Unexpected attachments
(files ending in .exe)

Suspicious links or links that don't match the destination



From: Banking Security Team (banking-security.support@gmail.com)

Subject: Urgent - Account Termination

Dear account holder,

You are required to update your account information immediately to prevent account termination.

Please follow the link below to update your password and verify your email address.

www.bankingsecurity.com/support

<http://www.malware.com/hacked.php>

Please read the updated privacy policies in the attached document.

Banking Support Team.



[privacy-doc-banking.exe](#)

**6
Ways
to Spot a
Phish**

