welltel

STAY SAFE ONLINE

Become Cyber Aware

PHISHING ATTACKS

Phishing emails look like they come from a trusted source and can often contain personal information. They may try to trick you into revealing information or can contain malicious links.

WHAT TO WATCH OUT FOR

1.**Don't trust the display name.** Check if the source is from the correct email address by comparing the display name with the sender's actual address.

2.**Watch out for urgent language** designed to make a person act before they've given time to consider is the email legitimate.

3.**Beware of impersonalised salutations** Dear Customer, Dear Contact etc. ..

4.**Hover over web links** even if they appear correct - Don't click on any links in a suspicious email if you hover over the link it shows the real address.

5.**Watch for misspelt words or poor grammar**

6.**Legitimate emails will be properly branded.** Be alarmed if you see variants in the company name or logo.

Anyone could click on a phishing email even the boss! If it happens to you tell someone straight away to minimise potential risk.

PROTECT YOUR PERSONAL INFORMATION

Personal Identifiable information (PII) such as name, address phone number, date of birth, account numbers can be used by criminals to create legitimate looking phishing emails.

1.Be cautious about sharing personal information online

2.Review privacy settings on your social media accounts

SECURE YOUR DEVICES

All devices including mobiles, laptops, tablets and PCs can be exploited to steal personal information and can be vulnerable to malware if not adequately secured.

1.Don't ignore updates, they contain patches that keep your device secure. If you are prompted to install an update don't ignore it!

2.Lock your devices. Use a password, fingerprint or pin. It will be more difficult for a hacker to access the devices if it is locked especially if it gets lost or stolen.

3.Don't download unofficial applications or software from unknown sources.
Check with your IT team first.

4.Be careful what you plug into your device. Malware is frequently spread by criminals leaving unattended USPs on trains and in shops which someone finds and puts into their PC or laptop.

USE STRONG PASSWORDS

Create passwords that are unique and hard to guess! Use 2 step verification where available.

1. Use a memorable but strong passwords.

2.Combine random words or incorporate a symbol such as ! or * and a number sequence.

3. Mix capital and lower case LeTTeRs

4. Use 10 or more characters

5.Avoid using predictable passwords such as 'Password123'

6.If you are given option to enable two Factor Authentication (2FA) take it. It's an extra layer of security.

SHOUT IF CAUGHT OUT

Remember that anyone in a business can make a mistake. Cyber criminal are cunning and people can be easily fooled.
If it happens to you don't delay in notifying your IT team or manager.

1.Cyber scams and phishing emails can be tricky to spot. Ask for advice or support when you come upon something that feels suspicious.

2.Report any suspicious behaviour immediately - remember it can happen to the boss just as easily as you. You can do more damage by trying to hide the error.

3.Educate yourself. Take the time to learn and understand the pitfalls. The majority of attacks start with human error. The more you know the safer you are.