SURF LIFE SAVING
NEW SOUTH WALES

Introduction

During this COVID-19 pandemic crisis, personal health and contagion transfer are not the only dangers. Many scammers are taking this opportunity through cyber intrusion campaigns know as Phishing to compromise your personal details.

How to Recognise a Phishing Attack

Scammers use email and text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or other personal information. If they get this information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- Say they've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your account or your payment information
- Say you must confirm some personal information
- Include a fake invoice
- Want you to click on a link to make a payment
- Offer a coupon for free stuff
- Say you're eligible to register for a refund or a rebate
- Remember if it's too good to be true, it probably is

How to protect yourself from Phishing Attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it's a good idea to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats. Microsoft Windows Defender is free and works with all modern versions of Windows

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats. Don't keep putting off phone software updates

3. Protect your accounts by using multi-factor authentication. Some providers offer an extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:
    - Something you have — like a passcode you get via text message or an authentication app
    - Something you are — like a scan of your fingerprint, your retina, or your face

- Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password

4. Call your telephone company and put a password on your account. With phone number portability, it's much easier for scammers to steal your phone number. If they steal your phone number, they can get access to any new text messages, such as one-time login codes to access your bank. By putting a password on your account with your telecommunications company you can prevent phone number porting attacks

5. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What to do if you think you've fallen for a Phishing Attack

If you think you've fallen for a phishing attack, there are some immediate steps you can take;

1. Reset your passwords. If you have entered your password into a phishing site, scammers will use that password to try and login to your accounts. By immediately changing the password you can mitigate this

2. Force logout of all accounts. Most online services will have a facility to "log you out" of all your active sessions. If in doubt, contact your service provider

3. Inform your workplace systems administrator that you may have inadvertently entered your credentials in to a questionable site and ask for their advice; or make a report to the Australian Cyber Security Centre https://www.cyber.gov.au/report