10 Tips to Stay Safe Online

1. Secure Your Device

The easiest way for hackers to get into your accounts is by accessing your device and its treasure trove of stored information. Lock all devices with a unique password/passphrase and if possible, set it to erase data after too many attempts. It is best to have your device automatically lock after a minute or 2 of non-use and ask for a password every time it wakes up.

2. Shop Safely With Trusted Sellers

Before providing any personal information or money to an online store, take a few minutes to learn about their reputation. Check reviews, referrals or site comments to make sure you're in good hands. A Google search can reveal red flags that will save you from a potentially dangerous experience.

3. Learn the Markers of a Secure Site

Any site that involves money or your personal details should be secure. Look for URLs beginning with https: (the 'S' is for secure) and a padlock icon. Sites which have been through more extensive security checks will have a highlighted green URL. Both markers mean any details you submit are encrypted securely and cannot be intercepted by hackers.

4. Use A Safe and Protective Payment Method

Always pay with a service that protects your personal details and offers additional security. Services such as PayPal or major credit cards are able to recover your money if a transaction goes wrong. Beware of merchants who request unusual or confusing methods such as mailing cash or wire transfers.

5. Think Before You Share

Take a moment to double check before posting something online that could damage your reputation or come back at some time in the future to embarrass you. A simple admission or casual thought now may involve issues later. It could also make you a target for trolls and hackers, drawing you into a lengthy battle with high emotional and financial costs.

6. Tighten Privacy Settings

All social media platforms offer privacy settings. These settings let you decide who can see your content - from the general public to a select few, you can choose who sees what. You can also control what your friends can do with your content. As a general rule set your privacy to 'friends only', and set individual posts as public/limited as required.

7. Use a Long, Unique Passphrase

Passwords are old hat, passphrases are what you should be using now. A passphrase is 2 or more words combined in an easily remembered combination. Choose a passphrase that is not only hard to guess, but hard to crack. Include numbers, letters, uppercase and symbols. Make sure that each account is using a unique passphrase and don't write them down. If remembering them is an issue, use a secure password keeper program.

8. Always Check the Sender's Email Address

Before replying or clicking a link, check that the email address is legitimate. Slight misspellings or add-ons to a known company email usually indicate they are not the real sender. If something doesn't feel right, delete the email immediately and check with the company. Keep an eye on emails from financial institutions in particular.

9. Check the URL

The URL you see on the screen may be different from where the link takes you. Fraudulent destination URLs are designed to extract your personal and financial information before you discover something is wrong. Always type important URLs manually and take the time to inspect others using mouse hover where possible. If it doesn't look right, don't click.

10. Outsmart Phishing Attempts

Not all 'phishing' attempts come through email. Hackers may call you on the phone, SMS or redirect you to a website in an effort to steal information. They will pretend to be a company you know and often appear quite legitimate. If you are at all unsure then contact the company directly. Sometimes these attacks are purely random, with hackers seeing if you bite. Other times they may be directly targeted at you and know extra information about your company including other staff names and similar information.

Need Help? Then give us a call to help secure your computers:

Contact:

DP Computing

Ph:	**08 8326 4364**
Fax:	**08 8382 3785**
Mobile:	**0412 973 503**
Email:	**support@dpcomputing.com.au**
Web:	**www.dpcomputing.com.au**

DP Computing - Providing a reliable and proven service since 1993.