Top 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/code and if possible, set it to erase data after too many attempts. It's best to have your device lock automatically 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 giving any personal details or money to an online store, take a few moments to learn about their reputation. Check reviews, referrals or site comments to make sure you're in good hands. A quick Google 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 protections. 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 future-check before posting something online that could damage your reputation or come back to embarrass you. A simple admission or casual thought now may involve a lot of drama 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 that help you decide who can see your content. From public to a select few, you can choose who sees what. You can also control what your friends can do with your content. Set your privacy to 'friends only' as a general rule, and set individual posts as public/limited as required.

7. Use a Long, Unique Password

Choose a password that is not only hard to guess, but hard to crack. Include numbers, letters, uppercase and symbols for each of your important accounts. Make sure to use a unique password for each account, 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 hitting reply 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 your details. They'll pretend to be a company you know and often appear quite legitimate. If you are at all unsure, contact the company directly. These attacks are purely random, with hackers are putting out their line to see if you bite. If you don't, they move on.

GIVE US A CALL TO HELP SECURE YOUR COMPUTER:

TechGuy911
Complete Healthcare Solutions for your PC

Phone: 813-727-6457
Web: www.Techguy911.com
Email: Randy@Techguy911.com