Cybersecurity: Protecting Your Family in the Digital and AI Age

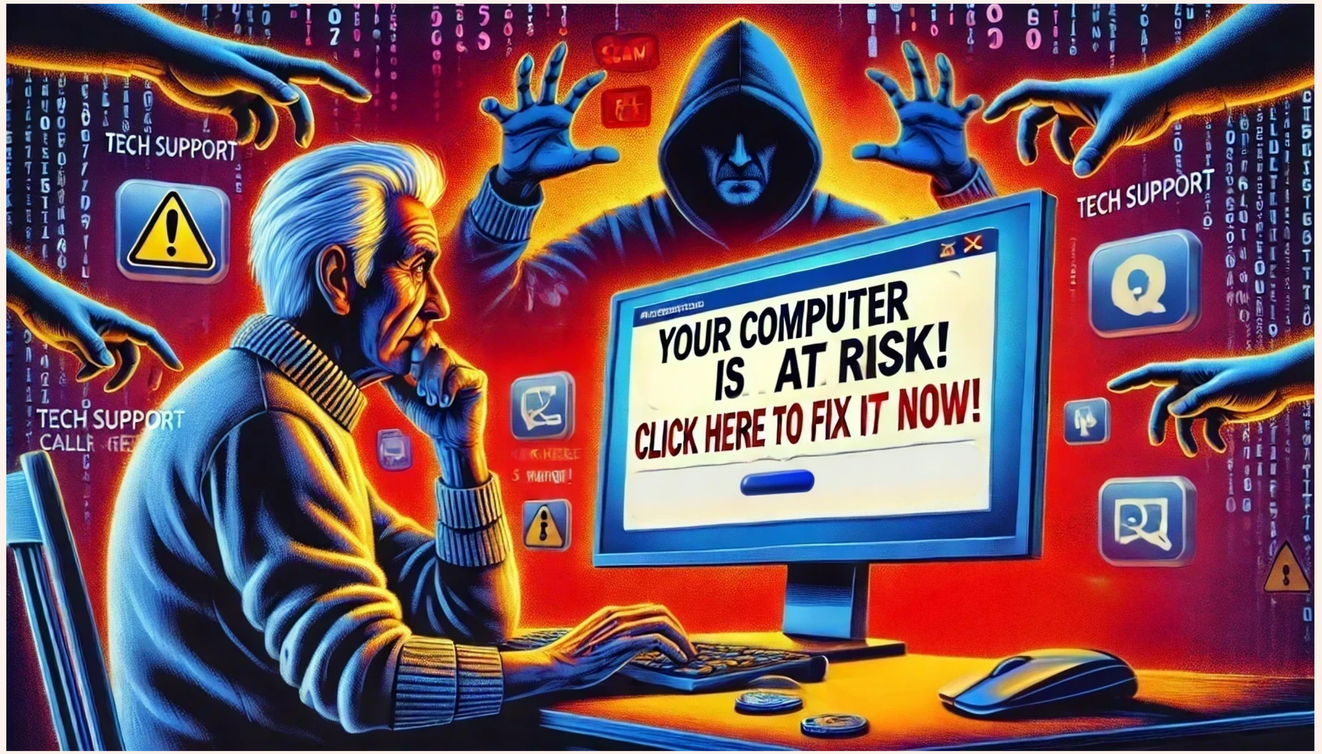

Illustration made by AI

Cybersecurity & Psychology

The World At Your Fingertips

We must reprogram how we think about threats because of the internet.

Prominent Targets

According to *The Media Trust Company*, criminals target a few specific groups of people:

Girls 13-14 years of age.

Males 17 years of age.

Seniors 75 years of age and older.

What are some signs that you may be facing an online scam?

Pressure to act quickly.

Unexpected requests for money, even from friends or family

Unsolicited contacts and requests for sensitive information

All of the above

The Science of Exploitation:
Emotional Manipulation and Time Urgency

Exploiting Trust

Is this person posing as an authority figure that has sought me out?

Fear Tactics

Am I being told I must do something immediatley to avoid a consequence?

Promises of Gain

Is this "opportunity" being presented as something I will miss out on if I don't "Act Now"?

Isolation and Desperation

Am I being promised an end to loneliness or recovery from a medical diagnosis or health issue?

Why are seniors often targeted by cybercriminals?

They typically have a higher net worth.

They are generally more trusting of

They may be less familiar with digital

They spend more time on-line, due to retirement.

What is the most common type of scam encountered by seniors?

Romance	Medical Treatment/ Drug	Tech Support/U pgrade	Utility Shutoff	Tax Payment	"Nigerian Prince" /Lottery

Common Scams

Phishing Scams

Phishing scams trick you into giving away personal info like your passwords or bank details. They often come as emails that look like they're from a legit company or bank. Always double-check the sender and never click on suspicious links!

Tech Support Fraud

This type of scam often begins with a pop-up window "alerting" you that software on your computer has expired, is out of date, or that it has detected a virus or malware and you need to grant remote access to fix it.

Romance Scams

Romance scams exploit the loneliness of those who've lost a spouse or are seeking one. They rely on decades of our comfort with giving out phone numbers to open the victim up to other types of scams.

What are some of the recommended practices to enhance your online security?

Practical Steps for Digital Protection

Create Strong Passwords

Use a mix of characters, numbers, and symbols to make passwords strong. Avoid common words and use different passwords for each account. Change them regularly.

Multi-Factor Authentication

Multi-factor authentication adds an extra layer of security. Even if someone gets your password, they need a second code, usually sent to your phone.

Beware of Phishing Scams

Don't click on suspicious emails or links. Phishing attempts can look legit. Always verify the source, preferably through a different medium.

Safe Browsing Habits

Visit only trusted websites and avoid downloading unknown files. Keep your antivirus software updated to protect against malware and viruses.

Reporting Channels

The Role of AI in Cybercrime

AI has lowered the threshold of skill required to perpetrate cybercrime. At present, it's being used to saturate the digital environment with threat vectors/traps at a rate legitimate authorities can't fully remove. That is changing, though...

Reporting Scams

If you suspect a scam, it's important to report it. Snap screenshots of any social media posts or texts, to keep records of any suspicious communications for law enforcement. Reporting helps prevent others from falling victim to similar scams.