Staying Secure in a Digital World — 7 Smart Ways to Stay Secure Today

Just 15 seconds of recorded speech is all it takes for advanced AI to replicate a voice with alarming accuracy. With capabilities this sophisticated, cybercriminals now have powerful tools to carry out impersonation scams, financial fraud, and other digital attacks. As these threats continue to evolve, now is the time to reassess your cyber habits to protect your identity, finances, and family.

Strong passwords alone aren't enough. This article offers a practical guide to the most common vulnerabilities individuals face — along with smart-solutions like burner phones, password managers, and cyber insurance options from top carriers.

Whether you're a client or a trusted advisor, taking proactive steps today can help ensure you're prepared for tomorrow's risks.

7 Cyber Vulnerabilities & Solutions

1.

Advertising Cell Phone Numbers: Personal cell numbers have become as critical as Social Security numbers for identity verification and access to banking, credit, and healthcare. Because these numbers are widely shared—from retail purchases to restaurant reservations—they've become a prime target for fraud and identity theft.

Solution: Use a "burner" phone number for low-priority transactions. Google Voice offers free numbers that can be set up in under ten minutes and managed through its mobile app. These numbers can send and receive calls and texts, keeping your primary number secure. [**Google Voice Link**].

2.

Traveling Abroad: Phones can be compromised when traveling in foreign countries, especially in regions where governments may be hostile to the U.S. or where surveillance is common. Your personal device may be subject to monitoring, malware installation, or data theft.

Solution: Consider purchasing a prepaid "burner" phone for international travel. These are available at major retailers like Target, Walmart, or online. Use this device exclusively for travel-related communication and avoid logging into sensitive accounts. And, as always, avoid public Wi-Fi, disable Bluetooth and use encrypted messaging apps such as Signal, etc.

3.

Engaging in Phishing Attacks: Phishing involves fake emails, texts or websites designed to trick users into revealing personal information or clicking malicious links. These scams often target payments by substituting banking details to divert funds to the fraudster's account. Common examples include fake toll payment requests from the Department of Transportation, impersonated Microsoft login prompts, and fraudulent Amazon delivery notifications.

Solution: Be cautious of repeated requests designed to create urgency and lower your guard. Never rely solely on payment details received via email—even secure emails warrant scrutiny. Always confirm sender information by calling a known, trusted phone number — do not use the phone number provided and avoid using search engines to find contact details, as scammers have created fake companies with convincing websites and phone numbers that appear in search results. To verify payment instructions, consider sending a small test amount first.

4.

Using Public WiFi. Public Wi-Fi networks can expose your data to cybercriminals who intercept traffic or mimic legitimate networks. This is especially risky during banking or other sensitive transactions.

Solution: Avoid using public Wi-Fi for banking or other sensitive transactions; in general, it's best to steer clear of public Wi-Fi altogether. Instead, use a cellular network for stronger security. Using a virtual private network (VPN) can also enhance protection by isolating your internet traffic from others on the network, though it doesn't eliminate all risks. A VPN helps ensure that data transmitted through the connection remains separate from other devices on the network. Finally, look for Secure Socket Layer (SSL) login pages whenever possible. SSL is a security protocol that allows websites to transmit sensitive information securely in an encrypted format. SSL-protected pages begin with "https://" instead of "http://" and typically display a lock icon to indicate a secure connection.

5.

Reusing Weak or Common Passwords: Using simple passwords or the same password across multiple accounts makes it easy for attackers to gain access.

Solution: Consider using a dedicated password manager like Dashlane or 1Password. These tools offer stronger security than the default password generators found on mobile devices. If your phone is compromised, any passwords stored or generated on it could be at risk as well. Also, be sure to use multi-factor authentication (verification to a cell phone or to an authenticator app) whenever offered for credit card, bank and investment accounts.

6.

Lack of Cybersecurity Awareness: Virtual schemes are on the rise. Without awareness, individuals may trust AI-generated content that appear professional but are designed to deceive.

Solution: Stay alert and establish a family codeword. If you receive an alarming- call, especially involving kidnapping or the exchange of money, contact local police immediately. If they're unresponsive, reach out to a 24/7 cyber hotline available through your cyber insurance or security provider.
By staying informed about common cyber threats and practicing smart digital habits, you strengthen your ability to protect yourself and your loved ones.

The more you learn, the more confident and prepared you become in recognizing and responding to potential risks.

EPIC

7.

Overlooking Protection: While taking proactive steps to protect yourself—like avoiding public Wi-Fi, enabling multi-factor authentication, and keeping software up to date—it's equally important to consider how to best protect yourself proactively and retroactively.

Solution: Proactive cybersecurity apps help you stay ahead of threats by detecting and blocking them before they cause damage. Whether you're shopping online, working remotely, or just browsing, these tools give you peace of mind and keep your digital life safe. Cyber Protection helps detect fraud early and may be available through your credit card or through various organizations. Lastly, for clients of AIG, Berkely One, Chubb, Cincinnati and PURE. Cyber Insurance coverage may be available. Coverage varies by provider, and it's important to note that losses involving cryptocurrency are generally excluded.

Policy Coverages	AIG	Berkley One	Chubb	Cincinnati	PURE
Forgery (forged signature or forged instructions)	$5,000, up to $100,000 by endorsement	$10,000, up to $50,000 by endorsement	$10,000	$10,000	$10,000, up to $1 million by endorsement
Identity Theft Expenses	$5,000, up to $100,000 by endorsement	$3,000, up to $20,000 by endorsement	$50,000	$100,000	$25,000
Identity Theft and Fraud Assistance	Cyber Scout, 888-760-9195	844-858-9583	866-860-1761	Cyber Scout, 877-432-7463	855-573-7873
Optional Available Coverages and limits available					
Online Extortion	$50,000 – $250,000	up to $100,000	up to $25,000		$100,000 to $1 million
Social Engineering (Intentional deception where you willingly transfer funds)		up to $100,000			$100,000 to $1 million
Cyberbullying	$50,000 – $250,000	up to $100,000	up to $250,000		
Data Restoration	$50,000 – $250,000	up to $100,000	up to $10,000		up to $100,000
Crisis Management	$50,000 – $250,000	up to $100,000	$50,000 – $100,000		$100,000 to $1 million
Active Monitoring	K2 Intelligence		Norton		Rubica

Avoiding cyber scammers requires constant vigilance, education, and immediate response by knowing who to call when there is a hint of fraudulent activity. Don't be caught unprepared — contact your EPIC Team with any questions.

Your team at EPIC Brokers is here to help. Contact your EPIC team today!

> "Keeping up with cybercriminals requires constant vigilance. Password managers, monitoring tools, and small test transfers for wiring requests help protect you and your assets."