Together with ciena

Stay Safe Online:
Essential Tricks and Key Tips

Introduction & Key Concepts

Whenever we leave our homes, we make sure to lock the doors and activate the alarms. Similarly, we roll up the car windows and take the keys when parking. And it goes without saying that we wouldn't share our ATM PIN with a stranger. In much the same way, when navigating the digital world, we need to adopt basic security practices to safeguard our personal and financial information.

No matter if you are a student just beginning to explore the internet, a consumer conducting online transactions, or a senior staying connected with loved ones via social media, these fundamental precautions are crucial for your cyber safety. This guide provides essential security tips and actionable advice for a secure online experience, allowing you to take full advantage of the internet's offerings with confidence and peace of mind.

Key Concepts

Becoming familiar with these online concepts is essential to protecting all of your private information:

Authentication

This is your digital identity card. Whether it's through passwords, biometric data (like fingerprints or facial recognition), or devices that generate or receive a unique code (two-factor authentication), these tools confirm it's really you.

Authorization

After confirming your identity, this process determines what files, resources, or areas of a network you are allowed to access. It's like having a key to certain doors in a building but not others.

Encryption

It's like turning your data into a secret code. Encryption transforms readable data into a scrambled format that can only be read by someone with the right decryption key (password or passphrase).

Hacking

Refers to the unauthorized intrusion into a computer or network. The hacker's intent can range from harmless pranking to stealing sensitive data, often involving malware to exploit vulnerabilities.

Firewalls

Your first line of defense in network security. Firewalls act as barriers to block unauthorized access to your network and permit outward communication, filtering out unauthorized or harmful types of data.

Malware and Viruses

Malware is software designed to harm or exploit any programmable device, service, or network. Viruses are a type of malware that replicate by inserting copies of themselves into other programs, files, or the boot sector of a hard drive.

Ransomware

This malware type locks or encrypts your data, effectively holding it hostage until you pay a ransom. It can infiltrate via deceptive links in emails, websites, or software applications.

Social Engineering

This is a manipulation technique that exploits human error to gain private information, access, or valuables. It often involves psychological manipulation, tricking unsuspecting users into making security mistakes or giving away sensitive information.

Virtual Private Networks (VPNs)

A VPN extends a private network across a public network, allowing you to send and receive data across shared or public networks as if your computing devices were directly connected to the private network. This ensures secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

Passwords

Passwords DO's and DON'Ts: Treat your passwords like the keys to your digital house.

DO	DON'T
Use robust, complex passwords.	Use easily guessable passwords such as "password" or personal information like birthdays or kids'/pet names.
Maintain unique passwords for different accounts.	Recycle passwords across different sites.
Utilize a password manager to generate and store passwords.	Write down passwords where others can find them.
Regularly update your passwords.	Share your passwords with anyone.
Enable two-factor authentication for added security.	

Avoid Phishing Expeditions

Phishing scams cleverly masquerade as trustworthy entities to steal your sensitive data. Protect yourself by:

- Checking sender's email addresses against official domains.
- Being wary of poor spelling, urgent requests, or suspicious links and attachments.
- Using updated security software to fend off malicious threats.
- Not succumbing to pressure tactics that demand immediate action.
- Reporting phishing attempts to help combat this form of cybercrime.

Stay Smart & Stay Secure: 9 Ways to Protect Your Digital Life

1 Update Regularly

Keep your operating systems, software, and apps up to date. Developers regularly patch security vulnerabilities with updates.

2 Be Wary of Links and Attachments

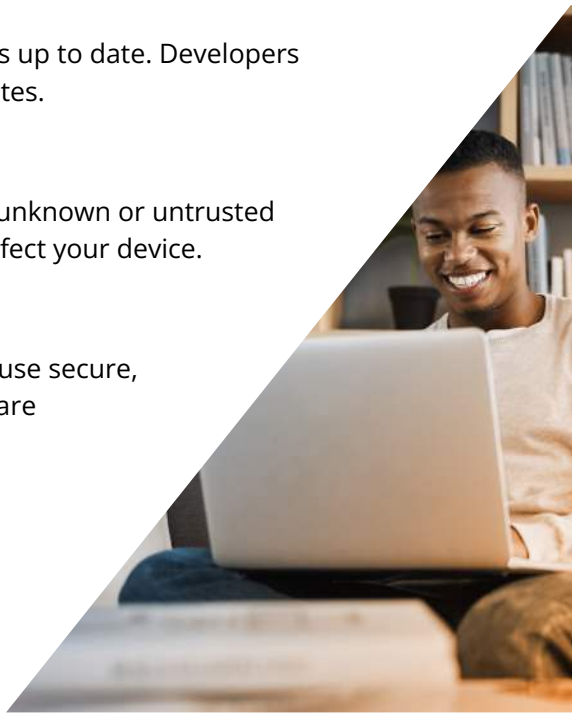
Exercise caution with links or attachments from unknown or untrusted sources. They can be gateways for malware to infect your device.

3 Use Secure Networks

When performing sensitive transactions, always use secure, private Wi-Fi connections. Public Wi-Fi networks are susceptible to security breaches, making your data vulnerable.

4 Back up Your Data

Regular backups to an external drive or cloud storage ensure that you can restore your data in the event of a cyber-attack or hardware failure.



5 Enable Privacy Settings

Control who sees what information on your social media and other online platforms. Set privacy settings to restrict access to personal information.

6 Secure Your Devices

Implement strong passwords, Touch ID, Face ID, or other forms of locks on your devices to prevent unauthorized access if they are lost or stolen.

7 Never Enable Macros from Unknown Sources

Macros can automate tasks in programs like Microsoft Office but can also be used maliciously to install malware. Be wary of documents that prompt you to enable them.

8 Be Skeptical

Approach unsolicited requests for your personal or financial information with suspicion. Verify the legitimacy of the request through official contact points.

9 Stay Informed

Educate yourself about the latest cyber threats and how to recognize phishing scams and other frauds. Staying informed helps you stay one step ahead of cybercriminals.

For more resources on maintaining online security, visit FTC's Identity Theft and Online Security page at https://consumer.ftc.gov/identity-theft-and-online-security.

About Zayo:

Since 2007, Zayo has focused on creating connections. By building an expansive network, Zayo has become the leading independent provider of light-speed data transmission infrastructure, with dense, high-quality networks connecting every major market in North America. Zayo was built to serve the largest and most innovative companies in the world, providing both major enterprises and individual internet users access to all the benefits the world wide web has to offer.

Together with ciena