clear MONEY

Staying Safe in the Digital World

Zing Credit Union
Realizing Possibilities

Keep a Clean Machine

- **Keep Security Software Current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats on your computer, phone, and tablet.
- **Automate Software Updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- **Protect All Devices that Connect to the Internet:** Computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- **Plug & Scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them before downloading or extracting files.

Protect Your Personal Information

- **Secure Your Accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- **Make Passwords Long & Strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Unique Account, Unique Password:** Having separate passwords for every account helps to thwart cybercriminals.
- **Sign Up for e-Statements:** 85% of identity theft cases start with stolen paper statements, bills, or checks (Javelin Strategy & Research, 2007). By viewing your statements through online banking, your personal and financial information is protected with multiple layers of security.
- **Keep Your Passwords Safe:** Everyone can forget a password. If you must keep a list, store them in a safe, secure place such as a password-protect password manager on your phone or computer.
- **Own Your Online Presence:** Set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how, and with whom you share information.

Connect with Care

- **When in Doubt, Throw it Out:** Links in emails, tweets, posts and online advertisements are often the ways cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email.
- **Get Savvy About WiFi Hotspots:** Limit the type of business you conduct when connected to a public wifi network by not accessing your financial accounts or any accounts containing sensitive information.
- **Protect Your Money:** When banking and shopping, check to be sure the sites are security-enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information ("http://" is not secure).

Be Web Wise

- **Think Before You Act:** Be wary of communications that instruct you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- **Protect Your Identity on Social Networking Accounts:** Use the least amount of information necessary to register for and use the site. Avoid sharing your date of birth, address, or contact information.
- **Stay Current, Keep Pace with New Ways to Stay Safe Online:** Check trusted websites such as the ones listed below to keep yourself informed and protected.

StaySafeOnline.org
Powered by National Cyber Security Alliance

STOP | THINK | CONNECT™