Top 10 online safety recommendations

Use the Lincoln Cybersecurity team's top 10 recommendations for staying safe online, a combination of behaviors and technology that can help protect you, your family, and Lincoln from cybercrime.

7% - 10%
of Americans are victims of identity fraud each year[1]

95% of cybersecurity breaches are due to human error[2]

Behavior

1. Develop a healthy level of paranoia.

Most cybersecurity experts trust little online — particularly email communications and anything that sounds too good to be true. Don't let fear paralyze you, but do maintain a healthy level of caution and skepticism.

2. Take ownership of your identity.

Identity monitoring is a must, and we strongly recommend credit locking, as well. Unfortunately, it's not a question of if identity theft may happen anymore, so own your Social Security number before someone else does.

3. Maintain control over social media.

Social media can be fun, but it also poses risks. Be smart about social media privacy and treat it like your next boss is following you.

4. Regularly monitor and place alerts on your accounts.

Make sure you watch your financial accounts, whether they're retirement plans, bank accounts, credit cards, brokerage activities, or other accounts. Enable auto-alerts and immediately respond to irregular activity.

5. Back up PCs regularly.

Cloud-based backup services are terrific for ensuring that the information on your PC can be restored, generally allowing you to "set it and forget it." Every so often, restore a file to make sure the backup function is working correctly.

Technology

6. Use two-factor authentication everywhere.

This identity verification technology is a cybercriminal's worst nightmare — and a must if you're using financial accounts, email, or anything that stores confidential information.

7. Auto-update all your devices.

Devices such as computers, tablets, and cell phones are constantly updating their software to address security vulnerabilities. Turn on auto-update for all your devices and security patches will be installed automatically for you.

[1] "Identity Theft and Internet Scams." Cybersecurity & Infrastructure Security Agency, October 2020, www.cisa.gov/sites/default/files/publications/NCSAM_TheftScams_2020.pdf.

[2] Milkovich, Devon. "15 Alarming Cyber Security Facts and Stats." Cybint, 23 December 2020, https://www.cybintsolutions.com/cyber-security-facts-stats/.

8. Enable all security features on mobile devices.

Fingerprint and face scans, five-try device lockdown, encryption, and other security features make sure your mobile devices are as secure as possible.

9. Protect your home network.

Always enable wireless security, keep kids off your PC, and consider services that can shield your home from malicious websites.

10. Use a password vault.

Most people today need to keep track of dozens of passwords. A password vault app is an effective way to manage them. There are several reputable vault providers to choose from, so make them part of your password strategy.

Check out in-depth cybersecurity resources to protect yourself at LincolnFinancial.com/CyberBasics.

Not a deposit
Not FDIC-insured
Not insured by any federal government agency
Not guaranteed by any bank or savings association
May go down in value

LincolnFinancial.com/Retirement

Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates.

Affiliates are separately responsible for their own financial and contractual obligations.

LCN-3458637-021821
PDF 3/21 **Z03**
Order code: DC-OSR-FLI001

Lincoln Financial Group®