Be Ready

Your health, wealth and cyber safety are our top priorities. As we continue to increase our use of digital tools and resources, it's important to take the right steps to keep your personal information secure. The Federal Trade Commission has released a number of ways people can protect themselves from cybercrime. Here are some of their top recommendations for staying safe online.

1. **Take ownership of your identity.** Identity monitoring is a must. Unfortunately, it's not a question of *if* identity theft may happen anymore, so own your SSN before someone else does. Make sure you watch your financial accounts, such as 401(k), bank, credit card, brokerage activity, etc. Enable auto-alerting and respond to irregular activity immediately. There are also identity theft protection services for more-robust monitoring you can use like LifeLock, IdentityForce, Identity Guard, and more.
2. **Don't just click.** Make sure you know who is asking for your personal information. Rather than clicking on an email link, visit the company's website and contact them directly to see whether a request was sent.
3. **Keep track of passwords.** 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, including Dashlane, LastPass, Keeper, and many more.
4. **Limit what you carry.** When heading out, take only the identification, credit and debit cards you need. Leave your social security card at home. Unless you are heading to the doctor, only carry a copy of your Medicare card and black out all but the last four digits.
5. **Shred 'em up.** If you don't need it, you should shred it. This includes receipts, credit card offers, checks, bank statements, expired credit cards, physician statements, insurance forms and other similar documents. Destroy prescription labels and be sure to not to respond to free health service offers.
6. **Consider opting out.** There are prescreened offers from credit card companies and insurance that are sent by mail. You have the option of opting out of these offers for five years or even permanently. To opt out, call 1-888-567-8688 or go to optoutprescreen.com. Nationwide credit reporting companies manage and operate the phone and website in a secure manner. Just remember that opting out permanently will remove some of the benefits from those offers.

CYBER SAFETY TOP 10 TIPS

1. Take ownership of your identity.
2. Don't just click.
3. Track your steps.
4. Limit what you carry.
5. Shred 'em up.
6. Consider opting out.
7. Ask before sharing.
8. Your social friends don't need to know everything.
9. Keep your devices secure.
10. When in doubt, freeze your account.

7. **Ask before sharing.** There are obviously institutions who will need your personal information – like your workplace, schools, doctor's office, advisor, etc. Ask why they need it and how they plan to safeguard it. When it comes to sharing your Social Security number, be sure to ask the following: *Why do you need it? How will it be used? How will you protect it? What happens if I don't share the number?*

8. **Your social friends don't need to know everything.** Social media can be fun, but it also poses risks. Be smart about social media privacy and don't post too much personal information about yourself. An identity thief can find information about your life, use it to answer security "challenge" questions and obtain access to your accounts. Do not share Social Security number, address, phone number, or account numbers. Be sure to limit access to your networks by reviewing the privacy options in the settings.

9. **Keep your devices secure.** Devices such as laptops, PC's, tablets and cell phones, are constantly updating their software to address security vulnerabilities. Turn auto-update on for all your devices and security patches will be installed automatically for you. Install anti-virus software, anti-spyware software, and a firewall. Be sure not to open files, click on links or download programs sent from strangers. Be wise about Wi-Fi too. If you use a secure wireless network and an encrypted website (look to see if there is a lock symbol before the start of the web address in the browser), the risk is lowered.

10. **When in doubt, freeze your account.** If you are concerned that your personal information has been exposed, shared in error or you think your identity has been stolen, we recommend credit freezing. Get more information from The Federal Trade Commission here.

If you have fallen victim to one of these phishing scams, please notify the Federal Bureau of Investigation by filing a report on their Internet Crime Complaint Center website, ic3. As always, please don't hesitate to reach out if you have concerns. We are here to help.

Please do not send any trading or transaction instructions through this email. They will not be honored or executed. Please call the Lincoln Financial Advisors trade desk at 1-800-237-3815.

If you do not wish to receive future e-mails from me, please call me at 617.728.7433, or e-mail me at Peter.Raskin@LFG.com.

Peter Raskin is a registered representative of Lincoln Financial Advisors Corp.

Raskin Planning Group is not an affiliate of Lincoln Financial Advisors.

Securities and investment advisory services offered through Lincoln Financial Advisors Corp., a broker-dealer (member SIPC) registered investment advisor. Insurance offered through Lincoln affiliates and other fine companies.

Lincoln Financial Advisors Corp. and its representatives do not provide legal or tax advice. You may want to consult a legal or tax advisor regarding any legal or tax information as it relates to your personal circumstances.

See Lincoln Financial Advisors (LFA's) Form CRS Customer Relationship Summary, available here, for succinct information about the relationships and services LFA offers to retail investors, related fees and costs, specified conflicts of interest, standards of conduct, and disciplinary history, among other things. LFA's Forms ADV, Part 2A, which describe LFA's investment advisory services, Regulation Best Interest Disclosure Document, which describes LFA's broker-dealer services, and other client disclosure documents can be found here.