Tips to keep you secure online

As you manage your finances and other details of your life online, it's important to be mindful of cyber threats.

	Do	Don't
 Passwords	✔ Use lengthy passwords, easy to remember for you but hard to guess for others; 8 characters minimum, but longer is recommended (e.g. passphrase or combination of characters) ✔ Change your passwords immediately if you suspect a site is compromised ✔ Turn on two-factor authentication when available ✔ Use password management software to protect and store your passwords	✘ Reuse passwords on multiple sites ✘ Share passwords with anyone ✘ Use personal information, common words, or generic passwords such as Password123
 Email	✔ Be suspicious of emails that ask for sensitive information or require immediate action ✔ Look for red flags, like urgent calls to action and misspellings, and generic salutations such as "Sir" or "Madam" ✔ Visit FBI's page on Scams and Safety and DHS's Stop. Think. Connect.™ Toolkit to learn more	✘ Assume an email is legitimate, even if it looks like it ✘ Discuss or email sensitive or financial information; if communicating with a legitimate organization, leverage encrypted messaging solutions to communicate more securely about personal matters ✘ Download suspicious attachments or click unknown links
 Behavior	✔ Consider turning off geo-location on your mobile devices or apps when not needed ✔ Know who is on your social media "friends" lists ✔ Validate that webpages are encrypted (have an https:// or a padlock in front of the address) to better protect the information you transmit	✘ Overshare on social media—cybercriminals may use this information to send targeted emails ✘ Provide personal information when playing online games ✘ Fall for online dating romance scams—be cautious about predatory behavior
 Apps and devices	✔ Use the correct app or website to access banking, insurance, and social media services and always keep them up to date ✔ Consider separate devices for home and work ✔ Set parental controls and be careful about letting children use your devices ✔ Use fingerprint or face ID, if available ✔ In addition to anti-virus software, install spam-defeating firewall and anti-malware software ✔ Back up your data on a personal, external drive	✘ Use public or shared devices to access accounts with sensitive information ✘ Leave your devices unattended or unlocked ✘ Use the Internet of Things (IoT) without understanding the privacy risks. Examples of IoT are security cameras, smart TVs, and voice command devices ✘ Download programs and apps from non-reputable sources
 Wi-Fi	✔ Make sure that your home network can only be accessed with a strong unique password ✔ Use trusted cable and Internet vendors, and the most updated, encrypted secure network system, Wireless Protected Access 2 (WPA2) ✔ If you are on a work laptop, use your employer's Virtual Private Network (VPN)	✘ Automatically connect to public Wi-Fi hotspots (turn this feature off) ✘ Assume public Wi-Fi is safe; cybercriminals frequently create fraudulent Wi-Fi hotspots ✘ Conduct sensitive business on public Wi-Fi

Other proactive tips:

- Subscribe to a credit monitoring service and review your credit report at least annually. Credit Bureaus: Experian 877-284-7942, Equifax 800-465-7166, and TransUnion 800-916-8800
- Learn more about scam prevention from the Federal Trade Commission and Federal Deposit Insurance Corporation
- Report lost or stolen cards and account information to your financial institution immediately
- Set financial alerts via email or text message to monitor account activity
- Shred important documents and expired cards
- Sign up for Online Statements
- Remember, reputable organizations don't initiate requests to input passwords, PINs or personal information over email, text or phone. When in doubt, verify requests through another known channel.

Learn more at unionbank.com/privacysecurity

UnionBank®

8914589 (07/19)