Tips to help you stay cyber safe

UnionBank® The Private Bank

PASSWORDS

DO

- Use lengthy passwords unique to each site. Use a phrase or password that you will remember but is hard to guess; eight characters at a minimum, longer is recommended.
- Keep your passwords private; don't write them down. Leverage a password manager for personal use to randomly generate strong, unique passwords and store them securely.
- When available, use Multi-Factor Authentication (MFA)/ Two-Factor Authentication (2FA) along with your username/ password.
- If you suspect your account is hacked, immediately change your password for that account and for any other accounts that use the same password and contact the companies' security departments.

DON'T

- Don't use easily guessed or commonly used passwords (e.g., "password") or sequential characters ("12345," etc.).
- Don't choose passwords based on details shared on social media accounts (e.g., names of kids or pets).
- Never reuse your company password on personal sites, and never reuse any passwords on multiple sites.
- Don't share your passwords with anyone.
- Do not store or send passwords in clear text (i.e., text information that is not encrypted).
- Do not hard-code passwords into computer code.

EMAILS/PHONE CALLS

DO

- If a sender/caller asks for sensitive information (e.g., Social Security or bank account #s) or requests a financial transaction (wiring money, etc.), verify the authenticity of the request by hanging up and calling back via a known phone number, known contact or legitimate email address —not one provided by the caller or in the email.
- Slow down and review email messages carefully before responding; be extremely cautious about clicking links or downloading attachments from external emails or unknown senders.
- At work, be cautious of unsolicited phone calls, particularly those that claim to come from your firm. Hang up and call back on a known number or send an email. Avoid providing organizational information to unsolicited callers.

DON'T

- Don't automatically click on links or download attachments in emails.
- Never transmit or forward client, sensitive, or confidential information to personal or non-company email addresses.
- Don't let urgent calls to action, threats, or warnings in emails or phone calls pressure you into taking risky actions or providing sensitive information.
- Never use your company email or username to register for any non-work-related websites.
- Don't assume caller ID is always accurate. Cybercriminals can "spoof" (i.e., disguise) phone numbers to make them appear trustworthy.
- Don't provide mobile numbers to unknown callers as criminals can use this number for vishing (voice phishing).

MOBILE DEVICES

DO

- Use strong passwords and biometrics (e.g., thumbprint or facial recognition) when available to access mobile devices.
- Treat your mobile devices (laptop, tablet, phone) like cash: keep them secure at all times.
- Download software or apps from reputable sources and ensure automatic manufacturer software updates run as soon as prompted.
- Remove all information from your mobile devices before trading/selling them as they could contain sensitive data. If you lose your mobile device and have a work app on it, report it right away to your company's IT department.

DON'T

- Never leave your devices unattended, even when working from home. When traveling, keep them with you or locked in a secure place (e.g., a hotel safe, not in a car trunk).
- Don't automatically assume public Wi-Fi access points are safe; hackers frequently create fraudulent Wi-Fi hotspots. If you must use a public network connection avoid performing activities involving personal and/or sensitive information.
- Don't automatically connect your device to public Wi-Fi hotspots; turn this feature off.

WORKING REMOTELY

DO

- Understand the risks of Internet of Things (IoT) devices connected to the Internet such as video cameras, voice assistants, speakers etc. that may be susceptible to being hacked.
- Turn off voice-assistant devices (e.g., Amazon Alexa) when conducting business discussions.
- Change your Internet router's default password to your own custom password (your Internet provider should be able to assist you with this).
- Ensure that you regularly update your personal devices with the latest software updates.
- Perform work related tasks only on your company computer (e.g., email and Internet usage) and lock your screen when you walk away from your computer.

DON'T

- Don't give out your Wi-Fi password.
- Don't allow anyone else at home to use your work computer.
- Don't send proprietary or confidential information to a personal email address.
- Never take pictures or screenshots of screens displaying sensitive data from your personal devices.
- Don't print company documents remotely unless you have approval.

TRAVELING

DO

- Make sure anti-virus software is updated on your personal devices; you will have better protection in the event you accidentally download malicious software.
- If you do not need your laptop or other electronic equipment, then do not take them with you; leave them at home in a secure place.
- Be aware of your surroundings; some travel destinations may pose a higher risk of theft.
- Be careful about discussing sensitive business topics in public places. Also, be alert for people "shoulder surfing" (looking over your shoulder to try to get sensitive information or passwords from your laptop or mobile device screen), especially on business travel.

DON'T

- Don't assume public Wi-Fi is safe; use a reputable source (e.g., hotel Wi-Fi with password) and confirm the password directly with staff from the establishment.
- Don't automatically connect to public Wi-Fi; in device settings, turn the auto-connect feature OFF so the device does not automatically connect to unsecure Wi-Fi networks.
- Don't leave mobile devices unattended; keep them in a secure place such as a hotel safe when the devices are not with you.

SOCIAL MEDIA

DO

- Do an inventory of your "friends" to ensure that you truly know the people you are sharing information with.
- Check privacy settings on all social media and consider setting your accounts to "private" so you can control who has access to your posts and information.
- Be careful sharing personal information, such as birthdate, hobbies or where you work, online or on a mobile device. Criminals can use this data to create tailored phishing emails/calls that target you and others in your social network.

DON'T

- Don't overshare on social media.
- Don't accept friend requests from everyone who asks.
- Don't automatically meet or give money to people you communicate with online.
- Don't repurpose passwords from different social media sites in case the site is hacked.

At Union Bank, your privacy and security are our priorities. Learn the fundamentals of our online security practices designed to safeguard your information and financial assets. https://www.unionbank.com/privacy/online-security

MUB7461 (08/22)