Fidelity Executive Services℠

Safeguard your digital life

Cybercriminals are targeting executives—here's how to protect yourself.

Registering and managing an account

- ☐ **Register your credentials to log in** to NetBenefits® and other online accounts before a cybercriminal can.
- ☐ **Create unique usernames and passwords.** Avoid using your name or email address as a username; if your provider (for example, Microsoft) uses your email address, be sure to enable multifactor authentication. Don't reuse passwords, and avoid weak, commonly used passwords like 123456. Consider using passphrases like "I LOVE ice cream!" instead.
- ☐ **Consider using a reputable, secure password manager** protected with a strong, unique password or passphrase. Don't keep passwords stored in files saved on your electronic devices.
- ☐ **Periodically check your account activity** and associated documents for unauthorized activity. **Activate security alerts** to warn you about suspicious behavior or changes to your account.

Account login and transactions

- ☐ **Enable multifactor authentication when available,** particularly with your financial, email, phone, and social media accounts.
- ☐ **Provide your current mobile phone number and email address** to Fidelity and other institutions you do business with so that you can be contacted in real time in case of fraud or high-risk transactions.
- ☐ **Use biometrics where available,** such as Fidelity MyVoice® (call us to enroll), thumbprint, and facial recognition.
- ☐ **Be cautious about using public Wi-Fi** without a dedicated, encrypted virtual private network (VPN). **Use trusted devices for sensitive transactions.** Avoid conducting financial transactions using shared devices or unsecured networks.

Applying for and monitoring your credit

- ☐ **Periodically review your credit and freeze it** to prevent credit fraud. Check for any suspicious activity, including profile changes or transaction attempts, and review alerts you may receive. Temporarily unfreeze it when you need to apply for credit.

  Contact:

  – Equifax | **Equifax.com/personal/credit-report-services** | **800-685-1111**

  – Experian | **Experian.com/help** | **888-EXPERIAN (888-397-3742)**

  – TransUnion | **TransUnion.com/credit-help** | **888-909-8872**

Securing your devices

- ☐ **Call your cell phone provider to enable a PIN or passphrase** to prevent criminals from porting your phone to a new carrier or swapping their SIM card for yours.
- ☐ **Secure your mobile devices** before they're lost or stolen. Activate the PIN or lock functions for each device—set them to auto-lock, and enable remote lock and data wipe. Use the "find my phone" and Face ID or Touch ID features, if available.
- ☐ **Enable the auto-update feature for your operating system and apps.** Install antivirus software on all computing devices.
- ☐ **Back up your data** to a secure cloud location.

Scams, social media, and mail

- ☐ **Forward any suspicious emails to your cybersecurity team and then delete. Don't click any links.** Additionally, if you receive a call that you are not expecting or that you find suspect, hang up.
- ☐ **Watch out for scams.** Business email compromise; phishing via SMS/text, voice, or email; and email and social media impersonation are the most common ways cybercriminals take over accounts and defraud executives each year. If you are faced with one of these scams, stop all communications immediately. Never give an unverified individual remote access to your computer. Learn more about **business email compromise**.
- ☐ **Limit personal and company information** you share on social media. Fraudsters and cybercriminals often use this information to attempt to conduct social engineering attacks.
- ☐ **Sign up for USPS Informed Delivery®, FedEx Delivery Manager®,** and **UPS My Choice®** to protect your mail.

870233.6.0 0622