



Fidelity Executive Services<sup>SM</sup>

# Safeguard your digital life

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

REGISTERING AND MANAGING  
AN ACCOUNT

ACCOUNT LOGIN  
AND TRANSACTIONS

APPLYING FOR AND  
MONITORING YOUR CREDIT

SECURING YOUR  
DEVICES

SCAMS, SOCIAL MEDIA,  
AND MAIL



## Registering and managing an account

- Register your credentials to log in** to NetBenefits<sup>®</sup> 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<sup>®</sup> (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](https://www.equifax.com/personal/credit-report-services) | 800-685-1111
- Experian | [Experian.com/help](https://www.experian.com/help) | 888-EXPERIAN (888-397-3742)
- TransUnion | [TransUnion.com/credit-help](https://www.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<sup>®</sup>, FedEx Delivery Manager<sup>®</sup>, and UPS My Choice<sup>®</sup>** to protect your mail.



Fidelity Executive Services<sup>SM</sup> does not provide tax or legal advice.

The information contained herein is as of the date of its publication, is subject to change, and is general in nature. Such information is provided for informational purposes only and should not be considered legal, tax, or compliance advice. Fidelity does not provide financial or investment advice. Fidelity cannot guarantee that such information is accurate, complete, or timely. Federal and state laws and regulations are complex and are subject to change. Laws of a specific state or laws that may be applicable to a particular situation may affect the applicability, accuracy, or completeness of this information. This information is not individualized, is not intended to serve as the primary or sole basis for your decisions, as there may be other factors you should consider, and may not be inclusive of everything that a firm should consider in this type of planning decision. Some of the concepts may not be applicable to all firms. Always consult an attorney, tax professional, or compliance representative regarding your specific legal, tax, or regulatory situation.

*Recommendation provided in this document is for informational and educational purposes only. To the extent any investment information in this material is deemed to be a recommendation, it is not meant to be impartial investment advice or advice in a fiduciary capacity and is not intended to be used as a primary basis for your or your client's investment decisions. Fidelity and its representatives may have a conflict of interest in the products or services mentioned in this material because they have a financial interest in, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or services, including Fidelity funds, certain third-party funds and products, and certain investment services.*

Our [Customer Protection Guarantee](#) reimburses you for losses from unauthorized activity in covered accounts occurring through no fault of your own.

The content provided and maintained by any third-party website is not owned or controlled by Fidelity. Fidelity takes no responsibility whatsoever nor in any way endorses any such content.

Third-party marks are the property of their respective owners; all other marks are the property of FMR LLC. Third parties referenced herein are independent companies and are not affiliated with Fidelity Investments. Listing them does not suggest a recommendation or endorsement by Fidelity Investments.

Personal and workplace investment products are provided by Fidelity Brokerage Services LLC, Member NYSE, SIPC.

NetBenefits, Fidelity MyVoice, and the Fidelity Investments and pyramid design logo are registered trademarks of FMR LLC.

© 2022 FMR LLC. All rights reserved.

870233.6.0

0622