SECURITY BASECAMP

Protect Your Financial Future

A GUIDE TO STAYINGAHEAD OF CYBERCRIMINALS

Fraud and cybercrime are increasing threats to your identity, data, and financial assets – **you don't have to be their next victim.**

CYBER SECURITY MATTERS

Today's fraudsters are more sophisticated than ever. They use phishing emails, fake websites, and even phone calls (vishing) to trick individuals into revealing sensitive information. Once they gain access, they may move money, place fraudulent trades, or steal personal identities.

Financial institutions and their vendors, including Security Basecamp—use advanced security protocols to protect critical information and assets. These simple tips can strengthen your firm and your clients' defenses and play a crucial role in safeguarding financial wellbeing.

SECURITY BASECAMP IS DEDICATED TO HELPING FINANCIAL FIRMS PROTECT THEIR CLIENTS

Security Basecamp follows industry best practices and custodian-recommended controls to safeguard your information:

Verification of all money movement requests.

Ongoing staff training in cybersecurity awareness.

Regular policy and procedure updates aligned with current threats.

TIPS TO KEEP YOUR ACCOUNTS **SECURE**

Always let your advisor know if you change your email, phone number, or mailing address.

Call your advisor immediately if you suspect any suspicious activity or believe your account may be compromised.

SECURITY BASECAMP

Protect Your Financial Future

SIX SIMPLE STEPS TO **STRENGTHEN YOUR CYBER DEFENSES**

STRENGTHEN YOUR PASSWORDS & LOGINS

- Create strong, unique passwords for each financial account.
- Use a password manager to store and generate secure credentials.
- Turn on two-factor authentication (2FA) for all email and financial logins.
- Avoid using personal details (e.g., birthdays, names) in passwords.

PROTECT YOUR DEVICES

- Keep operating systems and antivirus software updated on all computers, tablets, and smartphones.
- Avoid using public Wi-Fi for financial transactions unless you're connected through a Virtual Private Network (VPN).
- Back up your data to guard against ransomware regularly.

STAY ALERT TO FRAUD TACTICS

- Be wary of emails or texts that request urgent action or offer links to verify your identity. When in doubt, call the sender using a known number.
- Never trust wire instructions received via email without verbally confirming.
- Don't open attachments or click links from unknown senders—even if they appear legitimate.

SAFEGUARD YOUR EMAIL & ONLINE ACCOUNTS

- Use separate emails for financial and personal communications.
- Clean out old emails containing account or personal information.
- Enable alerts for suspicious login attempts or profile changes.

REVIEW & MONITOR REGULARLY

- Check financial statements and credit reports frequently.
- Consider placing a security freeze on your credit with all three major bureaus (Equifax, Experian, TransUnion).
- Report suspicious activity immediately to your advisor or institution.

SHARE LESS ONLINE

- Limit what you post on social media—especially birthdates, vacation plans, or financial milestones.
- Use privacy settings to control who sees your posts.
- Encourage your family members to be cautious as well—cybercriminals target the whole household.