ADVISER INVESTMENTS

5 CYBERSECURITY TIPS

KEEP YOUR INVESTMENTS SAFE

EMAIL PROTECTION

- Avoid saving any email containing detailed financial information, especially those containing account numbers or signatures.
- Be wary of emails that have a strange address in the "from" field, include spelling errors or odd text, urge you to update your information or are making an offer that seems too good to be true.
- Don't click any links in a suspicious email.

PRECAUTIONS YOUR ADVISER SHOULD TAKE

- Make sure they have policies in place to screen for fraudulent communications seeking access to your accounts.
- Advisers should not send emails including account numbers or other personally identifying information (PII).
- Advisers should not ask you to send PII via unsecured email.

SAFEGUARDING FINANCIAL ACCOUNTS

- Review all credit card and financial statements as soon as they arrive.
- Avoid developing online patterns such as regular wire transfers that cybercriminals could replicate.
- Never access your financial accounts from publicly accessible networks such as libraries, coffee shops and airports.

'RANSOMWARE' SCAM

- Do not grant access to your financial and personal information to anyone you do not trust.
- Remember that representatives from Microsoft, Apple or other software providers will not call you to report problems.
- If you are victimized by one of these scams, start by calling your local police station to report the incident.

SOCIAL MEDIA SAFETY

- Never post your Social Security number—even the last four digits.
- Consider keeping your birthdate, home address and home phone number confidential (i.e. keep them offline).
- Refrain from posting announcements about vacations, births and children's birthdays as it provides fraudsters information to pass authentication tests of your identity.

COMMON FRAUDS TO AVOID:

bonus

The Pigeon Drop: The right to large sum of money is promised in exchange for a “good faith” payment withdrawn from an individual’s bank account. Con artists will often employ an accomplice posing as a lawyer, banker or other seemingly trustworthy third party.

The Fake Accident: The con artist asks for a wire transfer or check to pay for a relative’s urgent medical care. This can be particularly convincing if the scammer has done his homework and researched the names of family members via social media. A similar scam involves calling to say a family member has been arrested and needs money for bail.

Charity Scams: Where money is solicited for bogus charities. These are especially prevalent after natural disasters.

IRS Impersonator: In this scenario, someone claiming to be from the Internal Revenue Service (IRS) calls to inform you that there is a problem with your tax return or that you owe taxes, and will threaten legal consequences (arrest, lawsuit, revocation of a driver’s license or deportation are the most common) to convince you to make an immediate payment. (An alternate version of this scam will have them claiming you are owed a big refund to lure you into sharing personal information instead of seeking payment.) The IRS will never call you if they haven’t first mailed a bill, and they will never demand immediate payment without allowing you to question or appeal what you owe. They will also never ask for a credit card number over the phone or require a specific form of payment like a prepaid debit card.

Questions?
Contact Adviser Investments at **(800) 492-6868** or email us at info@adviserinvestments.com.

ADVISER INVESTMENTS