CYBERWELLNESS℠ FRAUD ALERT

IMPORTANT:
Please read and act to keep your accounts safe

Recently we're seeing two different phone scams being perpetrated against our customers resulting in fraud – **here's what you need to know and do to protect your accounts.**

What to know

Remote Access Scams
Criminal claims to be from a well-known company and requests remote access to your computer, wanting you to believe you have a serious problem, e.g., a virus. Once on your computer, they install malware that captures all your keystrokes; or, they often ask you to pay a ransom or attempt to launder money through your account

Imposter Scams
Criminal calls you purporting to be from Fidelity Investments or another financial company, e.g., a bank, and requests you read back to them a one-time passcode that the criminal has generated through fraudulent web activity, e.g., a password reset.

Protect yourself

- No reputable institution will ever call you and request remote computer access or your account access credentials. If you get a call, **hang up.**
- If you receive a pop-up warning on your computer, **do not** call the number. Real security warnings **never** ask you to call a phone number.
- **Never** give away your passcode or password to anyone else.
- If you think your computer has a problem, update your security software and run a scan.
- If you're seeking technical support, go to a company you **know and trust**.
- **Report** it to the Federal Trade Commission and potentially affected account institutions

Resources to educate yourself

Fraud Alert Credit Freeze:
Equifax 800-525-6285
Experian 888-397-3742
TransUnion 800-680-7289

Federal Trade Commission How to Spot, Avoid and Report Tech Support Scams

For additional tips and resources, visit our Security Resources

Fidelity Investments Institutional Operations Company LLC, 245 Summer Street, Boston, MA 02210
938996.2.0

Fidelity INVESTMENTS