How to Prevent **Account takeover and Identity Theft**

Information

Account takeover occurs when an attacker gains unauthorized access to a user's account and assumes control of it, often without the user's knowledge. The attacker may use stolen login credentials (such as username and password) to access sensitive accounts like email, bank accounts, social media profiles, or any other online services. Once they take control, attackers can exploit the account for malicious purposes, such as identity theft, financial fraud, or spreading misinformation.

Identity theft occurs when someone acquires a piece of personal information and uses it to commit a crime.
Offenses involving identity theft are on the rise. These are the crimes most frequently reported to the Federal Trade Commission today.
Fraudsters commit these crimes in person, by telephone, on the Internet, or through the mail.
As technology continues to evolve, criminals are developing new ways to exploit or defraud organizations and consumers.
This includes attempting to access bank and brokerage accounts online and steal credit information or identities.
Wedbush Securities is diligent in its efforts to protect customers' information.
As part of our ongoing commitment to safeguard your privacy, we continuously review and strengthen our security program, processes, and procedures.

Background /Details

Wedbush Securities invests in technology and processes to ensure a secure electronic environment for all of your financial transactions, data transmissions, and communications. However, online security and protection of your identity and personal information is a team effort.
That's why we recommend you take steps to shield yourself and your computer from attempts to obtain your personal information electronically:

- Do not share your user ID or password with anyone. Wedbush Securities will never request your personal passwords or PINs
- Do not send or receive personal or account information through insecure or unencrypted email. Always respond via Wedbush Securities encrypted email service
- Use Client LINK online login to check your account balance and transactions regularly. Notify us immediately of suspicious account activity
- Never respond to, click any link in, or open an attachment in an email that requests information about you or your accounts. Wedbush Securities will never make such requests. If you accidentally click or respond to such requests, contact us immediately.
- If you are in doubt with any communication from Wedbush Securities, please call customer service to verify.
- Create Effective Passwords. They're an essential first line of defense in protecting yourself and your information.
  Do not use the same passwords for multiple services or websites or use passwords that can be easily guessed or discovered from public sources, like birth dates, addresses etc
- Be on the alert for Phishing, a process in which fraudsters try to commit fraud through illegitimate emails, text messages, and instant messages
- Use Spyware to protect your computer from dangerous software that distant hackers may use to extract sensitive information from your computer

Effective Passwords

Your identity is one of your most valuable resources. That is one reason why we want to help you take extra precautions to protect it. We recommend that you help safeguard your identity and personal information by using effective password protection. Here are some suggestions for creating safer passwords and some cautions against weaker ones.

- Avoid the use of personal information like birthday or a pet's name
- Don't choose passwords using dictionary words, names or parts of names, phone numbers, dates, etc.
- Choose passwords that aren't easy to guess
- Never share them or write them down
- Choose a different password for each account.
  For example, using the same password on bank accounts and social media may increase risk of identity theft or fraud
- Create passwords according to the website requirements
- Create original passwords that contain a combination of letters, numbers, and even special characters (#, &, %) if allowed
- Use both capital and lowercase letters (if your password can be case sensitive)
- Ensure that your passwords are at least sixteen characters
- Use a unique password for each service or website

- Choose a password you can easily remember, so you don't have to write it down
- Avoid using software that saves or remembers your passwords
- Change your passwords at least once a quarter

Phishing

"Phishing" refers to fraudulent processes in which fraudsters attempt to obtain your personal information through electronic communications, such as emails, text messages, or instant messages. These messages appear to be from a trustworthy entity, such as a bank, insurance company, retailer, or regulatory agency. However, the messages are not legitimate.
The fraudsters typically ask you to send your personal information to a website and then use that information to commit identity theft.

Remember, Wedbush Securities will never request personal information by emails, text messaging, or instant messaging.
Beware of any unsolicited emails that request personal information of any kind.
Do not respond to any such emails, texts, instant messages, pop-ups, or links. Instead, report this to ……

The following tips will help you spot fraudulent messages:

- The sender's name is usually generic, such as "Customer Service Department," or is just the company's name, such as "XYZ Securities/Bank."
- The message title generally concerns an "urgent matter" that requires your immediate attention, such as "verifying" certain information to prevent the company from suspending or closing your account
- The message may look professional and official, often displaying the look and feel of a website that you know. It may even contain links or pop-up windows that have the appearance of legitimacy
- The sender may ask for ATM or credit card numbers, personal identification numbers (PINs), sign-on IDs, and other personal information, such as your Social Security number, date of birth, or mother's maiden name -- all of which thieves can use to take over an account or commit identity theft
- The message may point you to a domain name that is spelled very close to or appears to be related to the legitimate domain name

If you are unsure of the origin of a Wedbush Securities email, or believe it is not legitimate, do not click on the links.
Instead, type wedbush.com URL in your browser's address bar.

Additional Resources

- Recovering from Identity Theft
- Identity Theft Resource Center
- National Cyber Security Alliance
- FTC Online Security Tips

Questions

- If you have any questions regarding Identity theft or Account Take Over, please contact Wedbush Securities at abuse@wedbush.com.