AB Information Security

Online Guidance for Clients

Preface

AB continually strives to be the most trusted investment management firm in the world and to offer client peace of mind. Consistent with these aspirations the enclosed guidance has been prepared to assist AB clients secure their personal online accounts[1].

Please forward any questions, concerns or feedback to:

Andreas Sobotta, Chief Security Officer
AllianceBernstein
501 Commerce Street
Nashville, TN 37203 U.S.A.
Email: **Andreas.Sobotta@alliancebernstein.com**

[1] Personal online accounts are defined as consumer home accounts utilized by the AB client. Examples include free internet mail accounts such as Apple iCloud Mail, Google Mail, Microsoft Outlook.com and social networking sites such as Facebook and LinkedIn.

How are online accounts hijacked?

Cyber criminals use a variety of methods to gain access to your online accounts with the most common being:

- *Password Guessing* – guessing simple passwords is a low-tech approach to gaining access to your personal online account. Hackers may use information about you to guess your password or use dictionary-based password guessing software.
- *Password Reuse* – cyber criminals may attempt to reuse your credentials (username and password) previously stolen from another website.
- *Social Engineering* – to trick you into disclosing confidential information, hackers may use deceptive techniques such as sending a familiar looking email (i.e., phishing email) with instructions to click on what appears to be a trustworthy hyperlink or to open a file attachment containing malicious software. Hackers also use SMS text messages with instructions to click on what appears to be a trustworthy hyperlink containing malicious software. This is known as smishing.
- *Malicious Software* – hackers may install malicious software on your computer to intercept your username, password and hyperlink information. In most cases, the malicious software is silently installed on your computer when you visit a compromised website, when you open a malicious file attached to a phishing email, or when you click on a malicious hyperlink enclosed within a phishing email.
- *SIM Swapping* - this technique involves a hacker convincing your mobile carrier to transfer your phone number to a new SIM card in their possession. Once the transfer is complete, the hacker can receive your calls and text messages, including any two-factor authentication codes sent to your phone, allowing them to gain access to your online accounts.

Online Guidance

AB recommends clients take the following action to reduce online risks:

1. Use **strong passwords**[i] designed to be hard for a person or a program to discover.
2. Avoid using the same password on multiple websites. Consider purchasing a consumer password manager (examples include Dashlane and LastPass) to secure your passwords to multiple websites.
3. Enable **multi-factor authentication** (also known as **two-factor authentication**) where available. Multi-factor authentication adds an extra layer of security to accounts by requiring users to provide two or more types of identification before they can access them. This could be something they know (like a password), something they have (like a special security device or a code sent to their phone), or something unique to them (like a fingerprint).
4. Review consumer website privacy settings to limit what the public can view about you.
5. Customize your web browser privacy and security settings to help protect from potentially harmful or malicious web content.
6. Where possible use separate email accounts along with unique and strong passwords for personal and financial communications.
7. Forward SMS text messages from an unknown sender to your wireless carrier at 7726 (SPAM). For more information go to https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages, https://about.att.com/pages/cyberaware/ae/smishing, or https://www.verizon.com/about/account-security/smishing-and-spam-text-messages
8. Use a commercial virtual private network (VPN) connection when connecting to the worldwide web over an unsecured connection like a public Wi-Fi hotspot. Examples include ExpressVPN and NordVPN. Avoid free VPNs as they are a security risk.
9. Ensure your personal computer is free of malicious software:
    a. Configure your computer to automatically install software security updates.
    b. Install antivirus software.
        I. Ensure the antivirus software automatically checks for updates.
        II. Schedule periodic antivirus scans to check for malicious software.
    c. Activate your computer's Internet firewall.
10. Microsoft customers should follow the security and privacy guidance provided by Microsoft at https://support.microsoft.com/en-us/security.
11. Apple customers should follow the security and privacy guidance provided at https://www.apple.com/privacy/manage-your-privacy, http://www.apple.com/macos/security and https://support.apple.com/guide/security/welcome/web.
12. Android customers should follow the security and privacy guidance provided at https://www.android.com/safety/.

Breach Guidance

AB clients who suspect their personal online account has been compromised are advised to take the following action:

1. On the compromised account:
    a. Immediately change the password to a new strong[i] password. Do not reuse a previous password.
    b. If the compromised account is an email account, check for message forwarding rules that may have been installed by the hacker without your knowledge.
    c. If possible, cease using the compromised account immediately.
    d. Enable multi-factor authentication (also known as two-factor authentication) where available. Multi-factor authentication adds an extra layer of security to accounts by requiring users to provide two or more types of identification before they can access them. This could be something they know (like a password), something they have (like a special security device or a code sent to their phone), or something unique to them (like a fingerprint)..
    e. Microsoft customers should follow the security and privacy guidance provided in the Microsoft Safety & Security Center at https://www.microsoft.com/en-us/safety.
    f. Apple customers should follow the security and privacy guidance provided at https://www.apple.com/privacy/manage-your-privacy, http://www.apple.com/macos/security and https://support.apple.com/guide/security/welcome/web.
    g. Android customers should follow the security and privacy guidance provided at https://www.android.com/safety/.

2. Other online accounts within your personal network:
    a. Change the passwords on all websites (e.g., email, instant messaging, online banking, social networks, shopping) using new strong passwords. The hacker may try to use the password stolen from your compromised account to login to other accounts within your network.
    b. Use website privacy settings to limit what the public can view about you.
    c. If you suspect that your online banking account has been compromised, immediately notify your financial institution.
    d. Where possible use separate email accounts (and strong passwords) for personal and financial communications.
    e. Be mindful that many online sites offer a self-service feature entitled “I forgot my password” which sends a temporary password to the accountholder’s personal email account. Once your email account is hijacked, it is easy for the hacker to obtain the password for your online sites linked to your email account.

Client Breach Guidance (continued)

3. Ensure your personal computer is free of malicious software:

For Windows:

a. **Run** Microsoft Update to download and install the latest security updates from Microsoft. Configure the update software to check for security updates automatically.

b. **Install** and **Update** anti-virus software. Configure the anti-virus software to automatically check for updates.

c. **Scan** the personal computer periodically for malicious software and remove. Configure the anti-virus software to automatically scan the computer for malicious software periodically. The **Microsoft Safety Scanner** can be downloaded from https://www.microsoft.com/en-us/wdsi/products/scanner

d. Turn on your personal computer's Internet firewall.

For MacOS:

a. **Run** Software Update to download and install the latest security updates from Apple. Configure the update software to check for security updates automatically.

b. **Install** and **Update** anti-virus software compatible with MacOS. Configure the anti-virus software to automatically check for updates

c. **Scan** the personal computer periodically for malicious software and remove. Configure the anti-virus software to automatically scan the computer for malicious software periodically. Consider using tools compatible with MacOS.

d. Turn on your personal computer's firewall. Go to System Settings > Network > Firewall and ensure it is enabled.

4. Purge old email messages containing confidential or personal information from your mailbox folders including inbox, sent items and deleted items. Where available, use the email export feature to copy the messages to a removable external hard drive before deleting. Remember to disconnect the removable hard drive from the computer when not in use.

5. If there is reason to believe that your address book or social networking site (e.g., Facebook, LinkedIn) has been breached, consider alerting family members and friends within your address book(s) as they may be targeted in the future by someone impersonating you.

6. If there is reason to believe that your identity is being used to perpetuate a fraudulent act involving a retail money wire transfer company such as Western Union, assume that your identity verification information has also been compromised and may be used by someone impersonating you in an attempt to withdraw the funds. Again, immediately notify your financial institutions of any suspected breach.

7. Refer to the consumer information offered by the U.S. Federal Trade Commission at http://IdentityTheft.gov

8. Strongly consider placing a **security freeze** on your credit files at Equifax, Experian, Innovis and TransUnion. Note that a **credit lock** is not the same as a freeze as the lock

does not prevent the credit bureaus from selling your credit reports to anyone requesting the information. For more information, refer to the FTC credit freeze FAQs at https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

9. Contact your AB Financial Advisor with any questions or concerns.

References

[i] **Strong Passwords**

A strong password is one designed to be difficult for a person or a program to discover. Because the purpose of a password is to ensure that only authorized users can access resources, a password that is easy to guess can expose your personal and your company's internal and confidential information. Essential components of a strong password include sufficient length and a mix of character types. When people create passwords, they often defeat the purpose by choosing parts of their names, the names of their pets, or even the word "password." A typical weak password is short and consists solely of letters in a single case. You can make your password much harder to break by using more characters, mixing upper and lower-case letters, and including numbers and special characters.

Below is guidance to assist you in creating a strong password:

- Password length – each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length.
- Combine letters, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess. A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection.
- Use the entire keyboard, not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.
- Use words and phrases that are easy for you to remember, but difficult for others to guess. People like to use passwords that will be easy for them to remember. It is suggested that you use a memorable phrase instead of a word, and convert that phrase to a password. For example, the phrase, "I have 2 puppies! Fido and Spot." could be expressed as Ih2p!F+S.

To avoid creating weak, easy-to-guess passwords:

- Avoid sequences or repeated characters. "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- Avoid using only look-alike substitutions of numbers or symbols. Malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.
- Avoid your login name or other identifiers. Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- Avoid dictionary words in any language. Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions.

For more information, refer to Microsoft's Online Privacy & Safety guidance at https://privacy.microsoft.com