Consumer eBanking Fraud Prevention Best Practices

Consumer eBanking Fraud Prevention Best Practices

User ID and Password/Passphrase Guidelines

- Create a "strong" password/passphrase with at least eight characters that includes a combination of mixed case letters, numbers, and special characters.
- Change your password/passphrase frequently.
- Never share user name and password/passphrase information with third-party providers.
- Avoid using an automatic login feature that saves user names and passwords/passphrases.

What makes a password strong?

Password strength is directly related to how much computing power is required to crack the password. Security experts recommend that users create long, complex passwords to exponentially increase the time it takes to crack. Here are some concrete steps you can take to improve the security of your passwords:

- **The longer the password, the better** – Experts recommend creating passwords that contain a minimum of 8 characters. If your password protects something sensitive, like access to your bank account, then use a minimum of 12 characters.
- **Use everything available on your keyboard** – Numbers, upper and lower case letters, and symbols all help to exponentially increase the strength of your password.
- **Throw away dictionary words** – You should never use common words or names within passwords. This rule can be extended one step further for those passwords protecting highly sensitive data to include compounds of multiple words. "IloveLabraDorReTrievers" is not a secure password if the information it's protecting is of high import.
- **Avoid commonly used password patterns** – A study by DARPA, the Defense Department's research agency, found that about half of all passwords used at a Fortune 100 company followed five common patterns, 3 of which are listed below:
    - One uppercase, five lowercase and three digits (Example: Komand123)
    - One uppercase, six lowercase and two digits (Example: Komando12)
    - One uppercase, three lowercase and five digits (Example: Koma12345)
- **Use unique passwords** – Don't cycle through the same set of passwords or recycle one across different services because that only diminishes the benefit of using a strong password. Research by Joseph Bonneau at the University of Cambridge shows that 31% of users reuse passwords in multiple places. When one of those reused passwords becomes compromised, the impact to the user is amplified.

Consumer eBanking Fraud Prevention Best Practices

- **Be careful where you store your passwords** – Do not store your passwords in spreadsheets or upload it to the cloud unless it's within an encrypted file. Our own data shows that the average company has 143 files on Microsoft's OneDrive that contain the word "password" in the file name. If you're going to store your password somewhere, use a reputable and secure password manager. Consumer Advocate website has a list of the 10 best password managers of 2020 to choose from. (https://www.consumersadvocate.org/password-manager/a/best-password-manager?)
- **Two-factor authentication is your friend** – This adds an additional layer of protection against hackers logging in with a stolen password. With two-factor authentication, the user must have her cell phone in order to verify her identity in addition to the username and password.

Consumer eBanking Fraud Prevention Best Practices

General Guidelines

- Do not use public or other unsecured computers for logging into Consumer eBanking.
- Check the last login date/time every time you log in.
- If the system does not recognize your computer or location, you will be asked to provide additional information to log into Consumer eBanking. This may include Out-of-Band Authentication via phone or SMS text message or answering more sophisticated (Out-of-Wallet) challenge questions.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.
- View transfer history available by viewing account activity information.
- Whenever possible, use Bill Pay instead of checks to limit account number exposure and to obtain better electronic record keeping.
- Take advantage of and regularly view system alerts; examples include:
    - Balance alerts
    - Password/Passphrase change alerts
    - Transfer alerts
- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Use the historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
- Never leave a computer unattended while using Consumer eBanking.
- Never conduct banking transactions while multiple browsers are open on your computer.

Consumer eBanking Fraud Prevention Best Practices

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as user names, passwords/passphrases, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail. Call the purported source if you are unsure who sent an e-mail.
- If an e-mail claiming to be from your financial organization seems suspicious, check with your financial organization.
- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.
- Ensure computers are patched regularly, particularly operating systems, browsers, and key applications.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Check your settings and select, at least, a medium level of security for your browsers.
- Clear the browser cache before starting any Consumer eBanking session to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.
- Be advised that you will never be presented with a maintenance page after entering login credentials. Legitimate maintenance pages are displayed when first reaching the URL and before entering login credentials.
- Consumer eBanking does not use pop-up windows to display login messages or errors. They are displayed directly on the login screen.
- Consumer eBanking never displays pop-up messages indicating that you cannot use your current browser.
- Consumer eBanking error messages never include an amount of time to wait before trying to login again.
- Be advised that repeatedly being asked to enter your user ID or s are signs of potentially harmful activity.

Consumer eBanking Fraud Prevention Best Practices

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router/access point) administrative password/passphrase from the factory default to a complex password/passphrase. Save the password/passphrase in a secure location as it will be needed to make future changes to the device.
- Disable remote administration of the wireless network hardware (router/access point).
- If possible, disable broadcasting the network SSID.
- If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.
- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.