

## Consumer eBanking Fraud Prevention Best Practices



Union Community Bank cares about our Consumer eBanking customers. We are providing you with these fraud prevention best practices to help you to avoid losses due to unauthorized access to your accounts. These practices are not intended to be all-inclusive; however, implementation of some or all of these guidelines should reduce the occurrence of online banking fraud.

### General Guidelines

- Create a “strong” password that includes a combination of mixed case letters, numbers, and special characters.
- Change your password frequently.
- Avoid using an automatic login feature that saves usernames and passwords.
- Do not use public or other unsecured computers for logging into Consumer eBanking.
- Check the last login date/time every time you log in.
- 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.
- Take advantage of and regularly view system alerts; i.e., Balance, Transfer & Password Change alerts.
- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Whenever possible, register your computer to avoid having to re-enter challenge questions and other authentication information with each login.
- Never leave a computer unattended while using Consumer eBanking.
- Never conduct banking transactions while multiple browsers are open on your computer.

## **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 usernames, passwords, 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.
- 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.
- 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.
- Clear the browser cache before starting any Business 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 repeatedly being asked to enter your password/token code are signs of potentially harmful activity.
- Being asked challenge questions if your computer was previously registered is a sign of potentially harmful activity.
- Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled.

## **Consumer eBanking Advisories**

- 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.
- Pop-up windows are not used to display login messages or errors. They are displayed directly on the login screen.
- Pop-up messages are not used to indicate that you cannot use your current browser.
- Error messages never include an amount of time to wait before trying to login again.