FINAL of Mobile Security FAQ's

What controls are used to prevent unauthorized access to my account?
Online banking and mobile banking use multifactor authentication to authenticate users at login.

How does Spectrum keep Online and Mobile Banking information (including login credentials) secure?
Our Online and Mobile Banking platforms do not store any information in the user's device or the Web browser cache. All data is securely transmitted to servers using Transport Layer Security (TLS).

Does Spectrum use challenge questions on the mobile channel?
No. Answers to challenge questions can be discovered or guessed easily. Instead, we use one-time passcodes (OTPs) sent out of band using SMS or phone calls.

Can users access the same functionality on mobile devices as they do on laptop or desktop computers?
No. To reduce risk, our mobile solutions do not allow risky activities such as changing profile information.

If my mobile device is lost or stolen, can anyone access his or her banking information or take over the account and identity?
No. If a member's mobile device or tablet is lost or stolen after authentication, the account cannot be accessed without the user name and password.

Stay safe, go paperless
Reduce the chance of mail fraud. Sign up for paperless statements by logging in to Online Banking.

Download apps only from trusted sources
Only download apps for your device on trusted sources such as the Apple App Store, Google Play, and Amazon Stores. This will protect you against fake and malicious mobile apps that may target your data.

Use mobile payment technology
Add your Spectrum debit or credit card into mobile payment apps that use tokenization – like Apple Pay®, Android Pay™ or Samsung Pay™. Every time you pay using the mobile payment app instead of using your physical card, you help to shield your card number from fraud.

Install software to find and remotely wipe your mobile phone
In the event your mobile device is lost or stolen, you should be able to remotely wipe your data to prevent unauthorized access. Install and configure an app that will let you remotely locate and wipe your phone (example: ‘Find My iPhone’ for iOS devices).

Bluetooth - If your device is Bluetooth capable, make sure 'Discoverable' mode is disabled. This prevents your phone from being detected by others scanning for Bluetooth devices in the area. This is the default setting on nearly all newer phones.

How can I protect my electronic devices?
At home and on the go, protect your electronic devices with these tips.

- Log off Online Banking or Mobile Banking when you have completed your transactions.
- Keep your Internet browser up-to-date with auto updates or:
    - Internet Explorer: Go to **Tools**, click **Windows Update** and follow instructions to download the latest patches.
    - Firefox: If you have an older version, click **Check for Updates** in the Help menu. For newer versions, go to **Options**, and the **Update** tab allows you to select how to check for updates.
    - Chrome: Click the Chrome menu and select **About Google Chrome**. The current version number is the series of numbers beneath the Google Chrome heading. Chrome will check for updates when you're on this page. Click **Relaunch** to apply any available update.
    - Safari: Keep Safari updated by keeping your system updated.
    - Keep your computer system and anti-virus software up-to-date with auto updates or:
        - Windows: Go to **Tools** in your browser. Click **Windows Update** and follow instructions to download the latest patches.
        - Mac: Choose **Software Update** from the Apple menu or set up automatic updates.
- Physically unplug from the Internet or shut down your computer when you are not using it.
- Do not store more personal information on your computer than is necessary, especially on laptops.
- Run anti-spyware software to remove any spyware from your computer or mobile device.
- Use spam filter software.
- Install a personal firewall or use your computer's firewall to help prevent unauthorized access to your home computer.
- Leave suspicious sites and do not follow instructions on them. For Internet Explorer (IE) users, you can adjust your browser security setting to Medium, a level that makes it more difficult for some malware to attack (select Internet Options from the Tools menu, then choose the Security tab).
- Browse safely - avoid using online and mobile banking on public WiFi networks.
- Educate yourself on Internet fraud with the Federal Trade Commission's Identity Theft section.
- Monitor your free credit report at least once a year.
- Look for the padlock symbol to see if a website is secure before you enter confidential personal information.
- Strong Passwords - Passwords keep others from getting into your personal information, so it is important to make them strong.
    - Change your Online Banking password regularly
    - Misspell a word or change a letter to a symbol.
    - Try using a phrase.
    - Avoid keeping a list of passwords by your computer.
    - Change your password immediately if you believe it has been compromised.
    - Do not give your passwords to anyone.
    - Check out these strong password resources.
    - Don't use the same password on multiple sites

- **Email**
    - Regular emails are not encrypted or secure. Anyone can read them. If you are emailing personal information, be sure to use our secure email options in PC Access and mobile banking.

    - Remember these tips when using email.
        - Do not reply to emails requesting or asking you to update your password, Personal Identification Number (PIN), credit or debit card number, Social Security number, or other personal information.
        - Delete spam (do not unsubscribe from it).
        - Avoid get-rich-quick offers.
        - Open an email and/or email attachments only when you know the sender. Spectrum will never send emails requesting personal information.
- **Fraud** - If you think someone is trying to get your personal information, or if you are worried you gave out too much information, report the incident immediately. Then change your passwords and monitor your account online to verify account transactions are valid.
- Balance your account at least once a month - Report any discrepancies in a timely manner.

What are the most common online security attacks?

The following are examples of how an unauthorized user may attempt to gain access to or exploit online and mobile systems:

- **Identity Theft** — The exploitation of a successful social engineering attack in which a person deliberately assumes the identity of another person for financial gain.

- **Phishing** — a form of social engineering characterized by attempts to gain access or personal information by impersonating a legitimate organization or individual, via e-Mail, instant message, or through a website.

- **Pharming** — the exploitation of vulnerabilities in the DNS servers that allows a hacker to acquire the Domain Name (e.g. “mycompany.com”) for a site and to redirect traffic from that company's legitimate site to the hacker’s website.

- **Viruses / Trojans** — malicious software intended to intercept or take control of a computer’s operation without the user’s consent. While viruses are typically used to destroy data or harm the computer, some are fairly benign while others are designed to capture personal information and transmit it back to the hacker’s web site.

- **Spyware / Keystroke loggers** — Similar to viruses and trojans, although typically spyware and keystroke loggers are not self-replicating. Used for capturing personal information without the user’s knowledge.

Where can I find additional information on security topics?

Internet Crime Complaint Center (IC3)

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. http://www.ic3.gov

NCUA Fraud Prevention Center

Visit the National Credit Union Administration's (NCUA) Fraud Prevention Center to learn how to recognize common scams, what you can do to protect your finances from fraud, and take action if you think you are a victim of fraud.
http://www.mycreditunion.gov/fraud/Pages/default.aspx

IdentityTheft.gov

IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. If you are the victim of identity theft, the site provides checklists and sample letters to guide you through the recovery process.
http://identitytheft.gov