CITIZENS

FRAUD UPDATE

RED,WHITE & BLUE

CELL PHONE CYBERSECURITY TIPS FOR YOU!

Smartphones have become the most popular electronic device that we use in our daily lives. It goes beyond making phone calls and sending text messages. We now use our smartphones as our own portable computers. In fact, many consumers say they use their phone in place of a personal computer. We run our lives from our smart phones and use them to schedule and organize appointments, track our fitness, pay bills, store card information on mobile wallet, send photos and videos to friends and family and so much more. Because we keep so much of our lives on our phones, it is so important that we keep our phones protected. Follow these security tips to help keep your cell phone data safe!

KEEP YOUR PHONE SOFTWARE UP-TO-DATE!

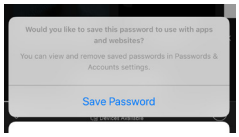
Hackers rely on vulnerabilities in mobile operating systems. If you continue to use old or obsolete versions of Operating Systems (OS), you risk exposing your mobile devices to security threats. OS updates provide fixes to possible bugs and security holes, along with cleaning up outdated software that may slow down your device.

KEEP YOUR SCREEN LOCKED

Protect your phone if it falls into the wrong hands. There are multiple types of lock screen protections you can use, PINS, unlock patterns, facial ID, and fingerprint. Any of these methods provide an extra layer of security, but make sure not to use overly simplistic patterns or PIN codes that would be easily guessable.

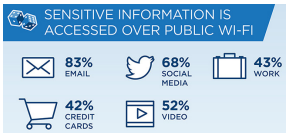
STRONG PASSWORDS

When setting up passwords for accounts, you will want to make sure there is a level of complexity. Do not make it something that would be easily guessable. Using different capitalization and special characters will help strengthen your passwords. You will also want to have unique passwords and not reuse the same password for all accounts. In the case of a data breach, having the same password on multiple accounts will leave you vulnerable.



BEWARE OF SAVING LOG-IN AND PAYMENT INFORMATION

Don't compromise security for convenience. Try not to use the "remember me" features for username/passwords and payment methods. Make sure you are setting up codes, PINS, and biometrics when using those features. Opt for using mobile wallet through Apple Pay, Samsung Pay, Google Pay, etc. for storing payment methods vs entering in the card data and saving for future use.



STEAR CLEAR FROM PUBLIC WI-FI CONNECTIONS

Try not to use public Wi-Fi hotspots. They are usually unsecured public networks and often do not include important security features and encryption. Using a VPN (virtual private network) connects you to an external server and masks your IP to hid your devices location.

Source:https://www.helpnetsecurity.com/2016/10/19/public-wi-fi-users-habits-risk/

Citizens BANK MINNESOTA
Member FDIC

WooHoo! Banking®

WooHoo! IT'S WHAT WE DO!

BLUETOOTH SAFETY

Bluetooth technology establishes a local network to exchange data wirelessly between nearby devices. Examples of this technology would be pairing earbuds to your phone, connecting your phone to the speakers in your vehicle, your fitbit to your phone, amongst many other devices. Bluetooth is a widely used technology today. While Bluetooth does have some security measures put in place such as; requiring connection approval and only pairing at short distances, you do need to be careful. Here are some tips on how to use Bluetooth safely.

1. **KEEP YOUR OPERATING SYSTEMS UP TO DATE** – Keeping all your apps and operating systems up-to-date is a very easy way to stay protected.

2. **MAKE YOUR BLUETOOTH DEVICE NOT DISCOVERABLE** – Make it hard for your device to be discovered by turning your device Bluetooth settings to "not discoverable" (How to do this will depend on your devices. Start by looking in your settings menu)

3. **DON'T SHARE SENSITIVE INFORMATION VIA BLUETOOTH** – If you need to send photos, passwords, login information, etc. use a secure way of transfer.

4. **BE CAREFUL WHO YOU CONNECT TO** – Be sure you know who you are getting a pairing request from. If you are unsure who is asking to pair for you and for what reason, decline or ignore the request.

5. **TURN OFF BLUETOOTH WHEN YOU ARE NOT USING IT** – When not using your Bluetooth, turn off your Bluetooth. It only takes a few short moments to reconnect, plus it will help save your battery life.

6. **DON'T PAIR IN PUBLIC WHEN POSSIBLE** – When connecting a new device, if possible, wait until you are at home or in a secure spot to do your initial pairings.

7. **UNPAIR DEVICES AS NEEDED** – Delete old Bluetooth pairing you no longer need or use.

RED FLAGS DO I NEED TO DO A SECURITY CHECK ON MY PHONE?

- **INCREASED DATA USAGE** – undetected viruses running in the background of your phone may significantly use more data than your normal activity.

- **FAST DRAINING BATTERY** – Similar to above, if there are viruses running in the background, the increase use of your phone's RAM may cause fast battery drainage.

- **DEVICE FEELS HOT** – Malware can consume RAM and CPU quickly, causing your phone to overheat.

- **UNAUTHORIZED CHARGES** – Some forms of trojans may trigger in-app purchases and text charges to premium accounts which hackers can then collect on.

- **UNUSUAL SEARCH ENGINES** – You probably have a primary search engine you utilize for searching such as Google, Safari, Bing, etc. If your searches are being answered by new or unrecognizable search engines, it could be a sign your phone has been infected by a virus.

- **POP-UPS** – while many free versions of apps contain pop-ups, if you start to experience increased pop-ups while your browser is closed, you may be experiencing adware, a type of malware that mines data.

- **INCREASE APP CRASHING** – If you have apps that are continually crashing, it is possible you may have a virus. Another common cause can be storage limits.

Each brand of mobile device has different ways of running security checks. If you have some of the red-flags listed above, you can get more information by going to that brand's website or calling your cell phone service provider.