Creating A Cyber Secure Home

As technology becomes increasingly important in our personal lives, so does the need to secure it.

Here are some fundamental steps you should always take to help protect yourself and your family.

1. Securing Yourself

Cyber attackers have learned that the easiest way to get something, is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true - it may be an attack.

Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing, as they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to create customized phishing attacks.

Another example might sound like this. Someone calls you pretending to be a Microsoft Support technician. They claim that your computer is infected, but actually are cyber criminals who want access to your computer. They may even try to convince you to purchase fake anti-virus software from them.

2. Securing Your Home Network

Your WIFI router is a physical device that controls who can connect to your wireless network at home.

To maintain the integrity of your network, always change the default administrator password on your WIFI router to a strong password that only you know.

Configure your WIFI network so that if anyone wants to join it, that person has to use a password. Additionally, always configure your wireless network to use the latest encryption - which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, smart TVs, wearable devices, and even some appliances.

3. Securing Your Computers and Devices

Here are some steps to protect any device connected to your home network.

Ensure all devices are protected by a strong PIN or passcode and are always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home. One for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged or administrator access.

Computers should have a firewall and anti-virus installed, enabled, and running the latest version of the software.

Before disposing of computers or mobile devices, be sure they are wiped clean of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

4. Securing Your Accounts/ Passwords

You most likely have a tremendous number of accounts online, that you access through your devices and computers. Here are some key steps to protecting them.

Always use long passwords that are hard to guess. Use passphrases when possible. A passphrase is a longer version of a password and is typically composed of multiple words, such as "MyFavoriteDessert".

Use a different password for each of your accounts and devices. If you cannot remember all of your strong passwords, we recommend you use a password manager to store them securely. A password manager is a computer program that securely stores all your passwords in an encrypted vault, so you only need to remember the password to the password manager program, and not to each account individually.

Use two-step verification whenever possible. Two-step verification requires a password and something else to log in to your account, such as a code sent to your smart phone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5. What To Do When Hacked

No matter how secure you are, eventually, you may be hacked.

To lessen the impact should this ever happen, create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you may be able to recover all of your personal information could be from those backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique one. If you no longer have access to any of your accounts, contact the financial institution immediately to let them know.

Monitor your financial accounts. If you see any charges you do not recognize, call the company you have an account with right away.

6. Take proactive steps to protect you and your identity

Identity theft is often a major goal for fraudsters and hackers. Here are some simple steps to proactively secure your identity and minimize the damage in the event you are hacked.

- Place a credit freeze with each of the major credit reporting bureaus. You can lift the freeze temporarily using their websites if you need to allow a legitimate credit check.
- Check your credit reports at least annually. You can obtain a free credit report yearly at https://www.annualcreditreport.com
- Monitor your credit score with our free SavvyMoney credit monitoring tool. Receive daily reports & notifications when changes are made to your credit score, or if any fraudulent activity has taken place.
- Set up notifications to stay on top of your financial account activity. Alerts can allow you to quickly identify and react to unauthorized account changes or transactions.

Did you know that 1 in 10 children aged 18 and under, have had their identity stolen? Most victims do not even know it!

Freezing your children's credit can be an important step in safeguarding their financial future. Each major credit-reporting bureau has free mechanisms for parents and guardians to freeze their children's credit until age 16. At 16, minors become eligible under federal law to monitor their own credit records, and will have to make their own credit freeze requests.

It is never too early to speak to your children about identity theft and financial literacy. If you have any questions or would like to inquire about how Arizona Central Credit Union can help plan for your child's financial future, please speak with a Member Service Associate at any of our branches, or call or email us at the numbers or email address below.

Call (602) 264-6421 or toll free at (866) 264-6421 or email us at solutions.center@azcentralcu.org

Revised: 2/2022

arizona central CREDIT UNION

CO-OP ATM

NCUA

Federally Insured by the NCUA

EQUAL HOUSING OPPORTUNITY