

Smart Devices 101

2019 FCE Leader Lesson

Sarah Ransom, FCS Agent in Johnson County

Goal of Lesson:

- To inform members about smart phone usage among older generations
- To discuss reasons for having a smart phone
- To educate about ways to remain safe while using a smart phone

Lesson:

Technology is something we hear about frequently. The younger generations are constantly keeping up with the latest releases and newest gadgets, but keeping up is never as easy as it may sound. Seniors, adults over 55, are consistently coming in with lower rates of technology adoption than the rest of the general public; however, they are more digitally connected than ever before (Pew Research Center, 2017). In 2017, it was reported that 4 out of 10 seniors own smartphones and this number is constantly on the rise. Starting at 17% of individuals 80 and older owning a smartphone, the numbers just increase as the age gets younger and younger. According to Pew, 80% of adults 65 years old+ own a cell phone, and of that, over 40% have a smart phone. With smart phone usage rising, the need for easy hands-on tips and safety is becoming very important.

Some of the benefits of using a smart devices include connecting and communicating with family and friends, participating in activities, making travel arrangements, getting medical advice and storing medical information, online shopping and banking, and mobile pictures. Even though there are great benefits, please remember a few tips for safety.

1. Use strong passwords – do not share with anyone other than a designated individual. This helps protect you against scams. If you keep multiple different passwords, have a safe location you keep these stored so you do not forget your passwords. Keep passwords at least 8 characters – make sure they include numbers, upper and lowercase letters and symbols. The more varied your password, the higher your security.
2. Use privacy settings – most of your services and apps provide controls that allow you to set who can see the things you post or share. You can limit who sees what information, which keeps the general public from knowing everything you are sharing with close family and friends. Before you share something on social media, be sure to check your privacy settings. Many smart devices have privacy settings on them, so you can protect your location, contacts and other personal information.
3. Deal with “spam”, abuse and unsolicited e-mails – this is annoying and can be very dangerous. Many of these lead to scams. The best thing to do is just delete them, do not open them and do not respond. Do not click on any links within e-mails like this because they usually lead to a scam or infect your device with malicious software. If someone is using threatening, mean, angry or accusatory language over social media, don’t respond and report it as abuse. Be sure to reach out to someone you trust to get additional help and support in reporting the situation.
4. Scammers are on the internet – it is not just phone calls where people are pretending to be someone they aren’t. The internet is full of people looking to take advantage and make a few extra dollars or steal identities. Be careful. If something seems fishy, follow your gut! Be aware of these specific scams that have been used a lot in the last few months:

- a. Personal emergency scams – scammers send messages appearing to be from someone you know, saying they are in trouble (wallet stolen, been arrested, etc.)
Call the person directly to see if this is true, or verify the information before you respond to that message. If it’s false information, report them and don’t respond.
 - b. “You owe money” scams – many scammers pretend to be a bill collector, IRS or family member who you owe money too. Don’t respond. Verify this information with the actual source. Never send them money until you have verified the information with an in-person, agency representative or agent.
 - c. Online dating scams – while there are great people on these, scammers also use these as ways of getting money from their romantic partner.
 - d. Infected computer scams – pop-up messages or phone calls from scammers may say your computer is infected or vulnerable to hacking. If this is phone call, hang up. If it is a pop-up message, close the browser and don’t click any buttons.
Reputable companies never make these calls. Responding in any way opens the door for the scammers to steal your money and plant viruses. Never download anything that is not from a legitimate source you are familiar with.
5. Click Carefully – when opening e-mails, purchasing online or browsing on your phone, be cautious. Read before making selections so you are not making decisions accidentally.
 6. Never send identifying personal information over text, email or internet – This can include your full birth date, social security number, bank accounts, etc. The only exception is bank accounts, loans or medical. Be sure to make sure you are on a secure site from a legitimate organization.

Using smart devices also opens up a world of possibilities – see the Connect Safely Guide for additional information. It can be found online at <https://www.connectsafely.org/wp-content/uploads/Seniors-Guide-to-Online-Safety.pdf>

References:

Connect Safely (September 2016) The Senior’s Guide to Online Safety.

<https://www.connectsafely.org/seniors/>

Pew Research Center (May 2017). Technology use among seniors.

<http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/>