Online Safety for Seniors
2 Stories

Hi, do you know me?

Hackers are professionals. They work hard creating new ways to trick seniors and teenagers. My friend Connie had a stranger call her landline and say: “Hi Grandma, do you know who this is?” Connie thought he sounded like her grandson and guessed: “Aiden?” The hacker played along, saying: “Yes!” and asking generic questions like “How’s church?” and “How’s the house?” Because her Facebook profile picture shows her wearing a Clemson University hat, he knew she’d be delighted to discuss the recent Clemson game. Connie had no reason to suspect that he wasn’t really Aiden. No reason, that is, until he asked for money. “It’s for mom’s birthday gift! We’re all going in on it together, Grandma.” He suggested mailing a check to an address she’d never heard before, then wanted to talk her through wiring the money directly from her bank. Suspicious, Connie said: “I’ll call you right back” and hung up before the caller could argue.

What would YOU do if this happened to you? (Pick 1)

+ Call Aiden’s mom and confirm his real phone number.
+ If you’re friends with Aiden on social media, send him a message confirming the story.
+ Write down the phone number of the person who called. Show it to Aiden — did one of his friends pull that trick? It happens, especially on college campuses.
+ If the hacker called on a landline phone, call the phone company and ask them to block the caller. They’ll want to be alerted to nefarious activity.
+ Notify the police. If multiple people report the same crime from the same phone number, then the police may be able to catch the hacker!
+ **Never mail a check or give your bank account information to an individual. Only familiar, trusted organizations like the church or the electric company may have your checks. A hacker can easily copy your checking and routing number from your check and make thousands more.**
+ When you want to mail a financial gift to someone who isn’t a familiar, trusted organization, send a gift card instead of a check. Gift cards contain no financial information for a hacker to steal.

Go Cavs!

Last Thanksgiving, my dad wanted to watch the Cleveland Cavaliers basketball game. My Dad is a savvy guy — he founded a corporate events company and expanded it to seven offices nationwide over 35 years. He masters new technology quickly. You're not going to hoodwink him easily. But he really wanted to watch that Cavs game, and I don't have a TV. So, Dad started googling. He found what he thought was a free streaming site. He started signing up, and then the site said: "Enter your credit card number." Dad thought: "Isn't this site free?" The site said: "We just want to verify your identity." As the Cavs took the court, Dad hurriedly entered the credit card details, eager to see the start of the game. Sure enough, the site started charging an exorbitant monthly fee.

Remember:

+ Never trust a site with "free" in the url. http://freestuff.org? Nope.
+ Never enter your credit card details unless you're prepared to buy something.
+ Many sites DO use your credit card to verify your identity – but they'll tell you upfront exactly how much they charge, and it's $1 - $5, not a monthly fee.

What would you do if this happened to you?

+ At the bottom of every website, you'll find their legal information. Look for a "contact" link, a phone number, an email address, even a company name – any way to contact them and reverse the charge.
+ Call your bank or credit card company, tell them what happened and ask for help stopping the monthly charge.
+ Don't worry. Plenty of intelligent people fall for these scams. Companies deliberately obscure the fine print in order to confuse you and sell more stuff.

If this happens to you, then don't be ashamed! Scammers are professional con artists. You can protect others by sharing your story. Tell your friends, so that they won't fall for it too!

> Genesis 50:20, moral of Joseph's story:
>
> *"What you intended for evil, God intended for good."*