SOUTH CAROLINA FAMILY AND COMMUNITY LEADERS
Affiliated with National Volunteer Outreach Network, Country Women's Council, U.S.A.,
Associated Country Women of the World
and in partnership with Clemson University Cooperative Extension Service
SCFCL website: http://www.scfcl.com

Leader Training Guide

Scams Need to Scram

Objective:

1. Learn what to do to protect your computer's security and the types of Internet fraud.
2. Learn how to report types of fraud and how to get help.

Lesson Overview/Introduction:

Crooks use clever schemes to defraud millions of people every year. They often combine sophisticated technology with age-old tricks to get people to send money or give out personal information. They add new twists to old schemes and pressure people to make important decisions on the spot. One thing that never changes: they follow the headlines — and the money.

Your personal information is a valuable commodity. It's not only the key to your financial identity, but also to your online identity. Knowing how to protect your information — and your identity — is a must in the 21st century.

Lesson:

Computer Security

Scammers, hackers and identity thieves are looking to steal your personal information - and your money. But there are steps you can take to protect yourself, like keeping your computer software up-to-date and giving out your personal information only when you have good reason.

Update Your Software. Keep your software – including your operating system, the web browsers you use to connect to the Internet, and your apps – up to date to protect against the latest threats. Most software can update automatically, so make sure to set yours to do so. Outdated software is easier for criminals to break into. If you think you have a virus or bad software on your computer, check out how to detect and get rid of malware.

Protect Your Personal Information. Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about why someone needs it and whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Protect Your Passwords. Here are a few ideas for creating strong passwords and keeping them safe:

- Use at least 10 characters; 12 is ideal for most home users.
- Try to be unpredictable – don't use names, dates, or common words. Mix numbers, symbols, and capital letters into the middle of your password, not at the beginning or end.

- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies where you do business – thieves can use it to take over all your accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not ask you for your password.
- If you write down a password, keep it locked up, out of plain sight.

Consider Turning On Two-Factor Authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

Give Personal Information Over Encrypted Websites Only. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address. That means the site is secure.

Back Up Your Files. No system is completely secure. Copy your files to an external hard drive or cloud storage. If your computer is attacked by malware, you will still have access to your files.

Internet Fraud Scam artists defraud millions of people each year by using internet services or software with internet access to trick victims into sending money or giving out personal information. ***It is important*** to take steps to protect yourself from and report internet fraud.

Types of Internet Fraud
Common examples of internet fraud include:

- **Data breaches** - When sensitive data (personal or financial information) is leaked from a secure location to an untrusted environment at a corporate or personal level
- **Malware** - This involves dangerous software that is designed to disable computers and computer systems.
- **Phishing or spoofing** - When a scammer uses fake email, text messages, or copycat websites to try to steal your identity or personal information, such as credit card numbers, bank account numbers, debit card PINs, and account passwords
- **Internet auction fraud** - This involves the misrepresentation of a product advertised for sale on an internet auction site, or non-delivery of merchandise.
- **Credit card fraud** - When scammers fraudulently obtain money or property through the unauthorized use of a credit or debit card or card number

Report Internet Fraud
If you believe you have been a victim of internet fraud or cybercrime, report it to the Internet Crime Complaint Center (IC3) or by using the FBI's online tips form. Your complaint will be forwarded to federal, state, local, or international law enforcement. You will need to contact your credit card company directly to notify them if you are disputing unauthorized charges from scammers on your card or if you suspect your credit card number has been compromised.

How to Protect Yourself
Take these actions before browsing or shopping for products and services on the internet:

DO

- **Learn how to spot internet fraud** - Find out the warning signs of common fraud schemes, including phishing or spoofing, data breaches, and malware.
- **Know your buyer or seller** - If you don't know who you're buying from or selling to online, do some research.
- **Update your antivirus software and antispyware programs** - Most types of antivirus software can be set up to make automatic updates. If your operating system does not offer free spyware protection (programs to prevent software from collecting information about you without your consent), you can find inexpensive software to download from the internet or at your local computer store. But be careful of ads on the internet offering downloadable spyware. You should only install programs from a trusted source.

DON'T

- **Don't give out your personal information to anyone you don't trust** - Never provide it in response to an email, a pop-up, or a website you've linked to from an email or web page.
- **Don't keep your computer on all the time** - Leaving your computer running all the time will make it more prone to spyware and other attacks from hackers and identity thieves.

Phishing and Vishing
Scammers use a variety of methods to try to steal your personal and financial information. They often try to make you feel comfortable with giving up your sensitive information by spoofing trusted logos of legitimate companies in an email or by pretending to be a family member or friend on the phone.

Phishing
Phishing is when a scammer uses fake email, text messages, or copycat websites to try to steal your identity or personal information, such as credit card numbers, bank account numbers, debit card PINs, and account passwords. The scammer may state that your account has been compromised or that one of your accounts was charged incorrectly. A scammer will instruct you to click on a link in the email or reply with your bank account number to confirm your identity or verify your account. They will sometimes threaten to disable your account if you don't reply, but don't believe it. Legitimate companies never ask for your password or account number by email.

Report Phishing Scams
Forward phishing email messages to spam@uce.gov or file a complaint with the Federal Trade Commission (FTC). Include the full email header of the scam message in your report. Find out how to do this by searching online for the name of your email service and the words "full email header."

How to Protect Yourself
Here are some ways to protect yourself from phishing scams:

DO

- **Reach out if you're unsure** - If you believe that a company needs personal information from you, call the number from their legitimate website or your address book. Do not call the number or use the links in the email. Tell the customer service representative about the request and ask if your account has been compromised.
- **Turn on two-factor authentication** - If your account supports it, you can set it up to require your password and an additional piece of information (code sent to your phone or a random number generated by an app) when you log in. This protects your account even when your password has been stolen.

DON'T

- **Don't click on any links or attachments in the email** - Any links, attachments, or phone numbers that you click on may contain a virus that can harm your computer. Even if links in the email say the name of the company, don't trust them. They may redirect to a fake website.

Vishing and Smishing
Similar to phishing, vishing (voice and phishing) and smishing (SMS texting and phishing) scammers also seek to steal your personal information. However, these scams target your mobile or landline phone instead of your computer. You may be directed to call a phone number to verify an account or to reactivate a debit or credit card.

Report Vishing and Smishing Scams
If you have received one of these requests, report it to the Internet Crime Complaint Center (IC3). Your complaint will be forwarded to federal, state, local, or international law enforcement. You will need to contact your credit card company directly to notify them if you are disputing unauthorized charges on your card from scammers, or if you suspect your credit card number has been compromised. Victims of these scams could also become victims of identity (ID) theft. Visit IdentityTheft.gov to learn how to minimize your risk.

Online Security and Safety
The internet makes many everyday tasks faster and more convenient, like shopping and banking, but it's important to be safe and responsible online. Scammers use the internet to try to trick you into sending them money or your personal information.

REPORT CYBER CRIME
If you believe you have been a victim of an internet-related crime, report it to these government authorities:

- The **Internet Crime Complaint Center (IC3)** refers internet-related criminal complaints to federal, state, local, or international law enforcement. Keep in mind, you will need to contact your credit card company directly to notify them if you are disputing unauthorized charges on your card or if you suspect that your credit card number has been compromised.
- The **Federal Trade Commission (FTC)** shares consumer complaints covering a wide range of categories, including online scams, with local, state, federal, and foreign law

enforcement partners. It cannot resolve individual complaints but can give you information on the next steps to take.
- EConsumer.gov accepts complaints about online and related transactions with foreign companies.
- The **Department of Justice (DOJ)** helps you report computer, internet-related, or intellectual property crime to the proper agency based on the scope of the crime.

HOW TO PROTECT YOURSELF
Here are some ways to keep your computer and personal information safe when going online:

DO
- Learn how to spot common scams and fraud - Find out the warning signs of internet fraud, phishing, and other online scams.
- Update your computer software - Download the latest versions of your operating system, web browsers, and apps.
- Talk to your kids about being safe and responsible online - If you are a parent, help protect your kids online by teaching them about the risks.

DON'T
- Don't share your passwords or sensitive information with anyone you don't trust - Think about why someone needs it and if you can really trust the request. Laptop security is also important when using a portable computer in public to help prevent all your valuable information stored on it from falling into the hands of an identity thief.
- Don't use the same passwords for multiple accounts - Try to make your passwords unpredictable and avoid using names, dates, or common words.
- Don't give out personal information over unencrypted websites - When shopping or banking online, only use websites that use encryption to protect your information as it goes from your computer to their server.

Stay a step ahead with the latest information and practical tips from the nation's consumer protection agency. Browse Federal Trade Commission's scam alerts by topic or by most recent to see the latest Scams.

The latest Scam: Scammers create fake emergencies to get your money

July 3, 2018
Carol Kando-Pineda, Attorney, Division of Consumer and Business Education
"I lost my wallet and ID. I'm stranded — please wire money."
"Your grandson is being held in jail. He needs bail money right away."
Scammers try to trick you into thinking a loved one is in trouble. They call, text, email, or send messages on social media about a supposed emergency with a family member or friend. They ask you to send money immediately. To make their story seem real, they may claim to be an authority figure, like a lawyer or police officer; they may have or guess at facts about your loved one. These imposters may insist that you keep quiet about their demand for money to keep you from checking out their story and identifying them as imposters. But no matter how real or urgent this seems — **it's a scam.**
If you get a call or message like this, what to do?

- **Check it out before you act.** Look up that friend or family's phone number yourself. Call them or another family member to see what's happening. Even if the person who contacted you told you not to.
- **Don't pay.** Don't wire money, send a check, overnight a money order, or pay with a gift card or cash reload card. Anyone who demands payment in these ways is always, always, always a scammer. These payment methods are like giving cash — and nearly untraceable, unless you act almost immediately. If you sent money to a family emergency scammer, contact the company you used to send the money (wire transfer service, bank, gift card company, or cash reload card company), and tell them it was a fraudulent transaction. Ask to have the transaction reversed, if possible. Report the message or call at **FTC.gov/complaint.**

Lesson Summary:
Members should have learned the types of internet scams, how to protect yourself against identity theft, how and where to report scams. The FTC and others have the most current list of scams to keep these issues readily available on their website.

Suggested Activities:
Watch this short video:
https://www.consumer.ftc.gov/blog/2018/07/scammers-create-fake-emergencies-get-your-money
Ask members to discuss a scam they have been involved in, what steps they used to take care of the issue and how the issue turned out.

Lesson Prepared by:
Pat Breznay, 2018-2020 SCFCL President

Lesson Reviewed by:
Christine J. Patrick, Food Safety and Nutrition Educator

Sources/References:
Federal Trade Commission, Consumer Information, Scam Alerts, consumer.ftc.gov
USA.gov, https://www.usa.gov/online-safety (844) USA-GOV1