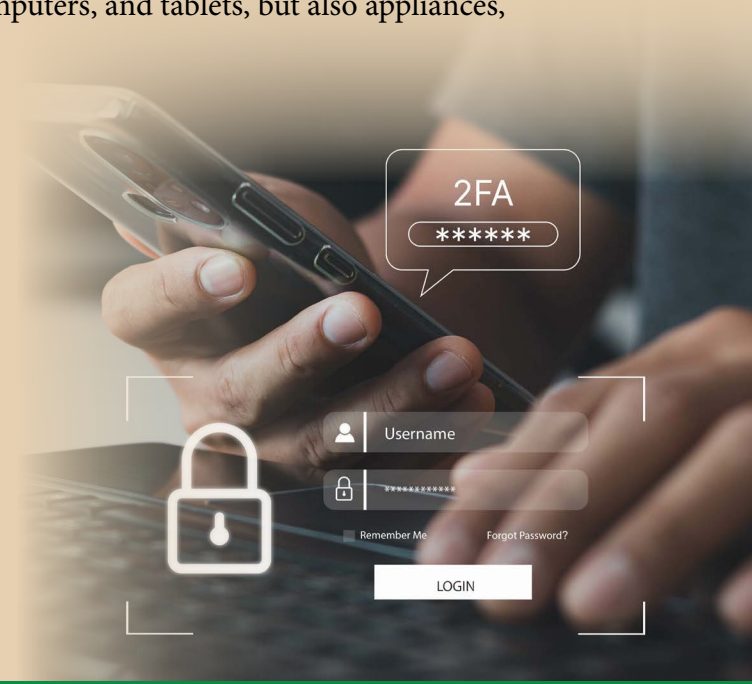
FLORIDA CONSUMER
NEWSLETTER
December 2023
A publication of the Florida Department of Agriculture and Consumer Services

PRACTICE GOOD CYBER HYGIENE

During the holiday season, cyber criminals will be hard at work looking to target online shoppers. The holiday shopping season is a prime opportunity for bad actors to take advantage of unsuspecting shoppers through fake websites, malicious links, and even fake charities. Their goal is simple: get a hold of your personal and financial information to compromise your data, insert malicious software, steal your identity, and take your money.

Cyber hygiene is a set of practices and steps that users of electronic devices take to maintain system health and improve online safety. Here are 4 common sense ways to practice good cyber hygiene and protect yourself online:

1. **Use strong passwords on your devices and accounts.** Once you've purchased an internet connected device, change the default password and use different and complex passwords for each device and account. Consider using a password manager to help generate and store unique passwords.
2. **Implement multi-factor authentication (MFA) on your accounts.** MFA authentication (or two-factor authentication) uses multiple pieces of information to verify your identity. Even if an attacker obtains your password, they may not be able to access your account if it's protected by this multiple step verification process.
3. **Update your software.** Before making any online purchases, make sure the device you're using to shop online is up to date. In fact, enable automatic software updates where applicable, as running the latest version of software helps ensure the manufacturers are still supporting it and providing the latest patches for vulnerabilities. This includes items like mobile phones, computers, and tablets, but also appliances, electronics, and children's
4. Think before you click. There are a lot of special offers during the holidays. Cyber criminals will often use phishing emails or social media posts—designed to look like they're from retailers—that have malicious links or that ask for you to input your personal or financial information. Don't click links or download attachments unless you're confident of where they came from. If you're unsure if an offer or a retailer is legitimate, type the URL of the retailer or company into your web browser as opposed to clicking the link.



Using strong passwords, turning on multi-factor authentication, updating your software, and thinking before you click on suspicious links are the basics of cyber hygiene and will drastically improve your online safety.

For more information on Scams and Fraud, visit www.FloridaConsumerHelp.com.

ONLINE SHOPPING: BREEZE OR BUMMER?

Online shopping can make checking off that holiday list a breeze. But what happens when your package doesn't come when the seller said it would? Or what if it never comes at all? All your holiday cheer can quickly turn to anger and frustration, and that can be a real bummer.
The federal Mail, Internet, or Telephone Order Merchandise Rule applies to most things you order by mail, online, or by phone. It says:

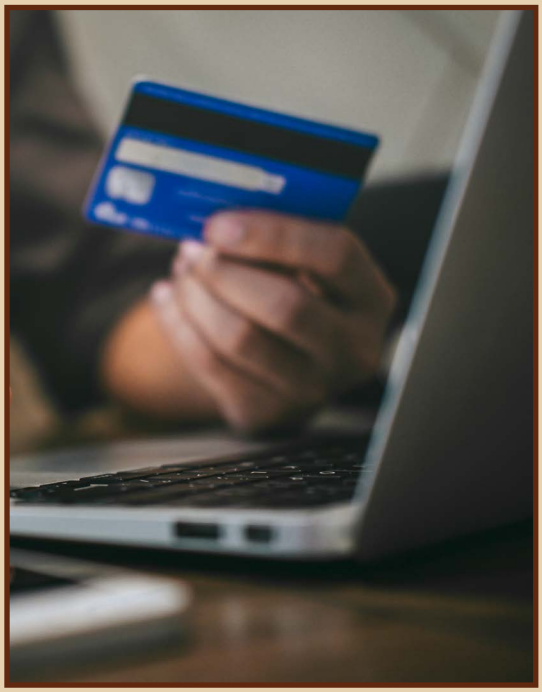
- Sellers must ship your order within the time they (or their ads) say. That goes whether they say "2-Day Shipping" or "In Stock & Ships Today." If they don't give a time, they must ship within 30 days of when you placed your order.
- If there's a delay shipping your order, the seller must tell you and give you the choice of either agreeing to the delay or canceling your order for a full refund.
- If the seller doesn't ship your order, it must give you a full refund — not just a gift card or store credit.

Avoid online shopping headaches by following a few simple tips.

- **Check out the company.** Search online for the name plus words like "review," "complaint," or "scam." See what other people say about it.
- **Check out the product.** Read the seller's description of the product carefully. If expensive brand-name items are offered for bargain prices, they could be counterfeit or stolen. Be sure to verify the item's availability and the total cost before you place your order.
- **Check the seller's refund policies.** The seller should disclose whether you can return the item for a full refund. If you can return it, find out who pays the shipping costs for returns, how many days you have to return the item, and if there is a restocking fee.
- **Pay by credit card.** Credit cards give you some protections that other payment methods may not. If there is a problem, the law allows you to dispute charges and temporarily withhold payment while your dispute is investigated.
- **Verify the site is secure.** Before you enter your payment information, verify that the website address begins with "https." The "s" stands for "secure" and means that your information is encrypted before it is transmitted.

If you don't receive your order

- Contact the seller. Most businesses will work with you to resolve the problem and keep you as a customer.
- If you paid by credit card, dispute the charge. The Fair Credit Billing Act treats certain credit card charges that you dispute as billing errors. Billing errors include charges for items that you didn't accept or that weren't delivered as agreed, involved the wrong amount, were unauthorized, and certain others. By law, credit card billing errors must be disputed in writing within 60 days of the date that the first statement with the billing error is sent to you. Some card issuers let you dispute billing errors over the phone or online. However, to be sure that you get the full protection of the law, follow up with a letter.
- If you paid by debit card, contact your debit card company (often your bank or credit union). Ask if they can help you. The consumer protections for debit cards are different from the protections for credit cards. You may not be able to get a refund for non-delivery or delivery of the wrong item. Some debit card issuers may voluntarily offer protections. Start by calling the customer service number. Follow up with a letter.



A word on timing, as the holidays approach: online sellers are required by law to ship when they (or their ads) say they will. If they don't ship then, they must tell you and give you a chance to cancel and get a full refund. If they don't give a shipping date, they have 30 days to ship from the date of your order.

FBI WARNS OF "PHANTOM HACKER" SCAMS TARGETING SENIOR CITIZENS

The Federal Bureau of Investigations is warning the public of a recent nationwide increase in "Phantom Hacker" scams, significantly impacting senior citizens. This Phantom Hacker scam is an evolution of more general tech support scams, layering imposter tech support, financial institution, and government personas to enhance the trust victims place in the scammers and identify the most lucrative accounts to target. Victims often suffer the loss of entire banking, savings, retirement, or investment accounts under the guise of "protecting" their assets. Between January and June 2023, 19,000 complaints related to tech support scams were submitted to the FBI Internet Crime Complaint Center (IC3), with estimated victim losses of over $542 million. Almost 50% of the victims reported to IC3 were over 60 years-old, comprising 66% of the total losses. As of August 2023, losses have already exceeded those in 2022 by 40%.

THE SCAM

Phase 1 - Tech Support Imposter

1. A scammer posing as a tech or customer sup port representative from a legitimate company contacts the victim through a phone call, text, email, or a pop-up window on the victim's computer and instructs the victim to call a number for "assistance."
2. Once the victim calls the number, a scammer directs the victim to download a software pro gram, allowing the scammer remote access to the victim's computer. The scammer pretends to run a virus scan on the victim's computer and falsely claims the computer has been or is at risk of being hacked.
3. Next, the scammer requests the victim open their financial accounts to determine whether there have been any unauthorized charges - a tactic the scammer uses to determine which financial account is most lucrative for targeting. The scammer chooses an account to target and tells the victim they will receive a call with further instructions from the fraud department of the respective financial institution hosting that account.

Phase 2 - Financial Institution Imposter

1. A scammer posing as a representative of the financial institution mentioned in phase 1, such as a bank or a brokerage firm, contacts the victim. The scammer falsely informs the victim their computer and financial accounts have been accessed by a foreign hacker and the victim must move their money to a "safe" third-party account, such as an account with the Federal Reserve or another US Government agency.
2. The scammer directs the victim to transfer money via a wire transfer, cash, or cryptocurrency, often directly to overseas recipients. The scammer may instruct the victim to send multiple transactions over a span of days or months.
3. The scammer tells the victim to not inform anyone of the real reason they are moving their money.

Phase 3 - US Government Imposter

1. The victim may also be contacted by a scammer posing as an employee at the Federal Reserve or another US Government agency. If the victim becomes suspicious of the government imposter, the scammer may send an email or a letter on what appears to be official US Government letterhead to legitimize the scam.
2. The scammer continues to emphasize the victim's funds are "unsafe" and they must be moved to a new "alias" account for protection until the victim concedes.

TIPS TO PROTECT YOURSELF

- Do not click on unsolicited pop-ups, links sent via text messages, or email links or attachments.
- Do not contact the telephone number provided in a pop-up, text, or email.
- Do not download software at the request of an unknown individual who contacted you.
- Do not allow an unknown individual who contacted you to have control of your computer.
- The US Government will never request you send money via wire transfer to foreign accounts, cryptocurrency, or gift/prepaid cards.

REPORT IT

The FBI requests victims report these fraudulent or suspicious activities to their local FBI field office and the FBI IC3 at www.ic3.gov. Be sure to include as much information as possible.

- The name of the person or company that contacted you.
- Methods of communication used, to include websites, emails, and telephone numbers.
- The bank account number(s) where the funds were wired to and the recipient's name(s).

For additional information on similar scams, please see previous Public Service Announcements published on the FBI IC3 website.

- IC3 | Technical and Customer Support Fraud
- IC3 | Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies
  IC3 | Scammers Using Computer-Technical Support Impersonation Scams to Target Victims and Conduct Wire Transfers

BAKING SAFETY THIS WINTER SEASON

The winter season brings delicious homemade goodies like cookies, cakes, and breads. If you enjoy making holiday treats from scratch using raw ingredients, here are a few important tips to help keep you safe from foodborne illness.

- Keep all raw foods, like eggs and flour, separate from ready-to eat foods.
- Keep raw eggs refrigerated at 40 °F or below until ready to use.
- Desserts containing eggs should be baked to a safe internal temperature of 145 °F.
- Follow package directions on baking mixes and other flour-containing products for correct cooking temperatures and times.
- Remember, flour is a powder that can spread easily.
- Wash your hands thoroughly for at least 20 seconds before and after touching raw ingredients.
- View more Baking Safety Tips here.

For more information on food safety, visit the Division of Food Safety's Holidays and Festivals website and the Division of Food Safety's Winter Food Safety website.

ABOUT THE FDACS DIVISION OF CONSUMER SERVICES

FDACS is Florida's state consumer protection agency responsible for regulating charities and handling consumer complaints. FDACS handles more than 400,000 consumer complaints and inquiries, oversees more than 500,000 regulated devices, entities, and products like gas pumps and grocery scales, performs over 61,000 lab analyses on products like gasoline and brake fluid, performs nearly 9,000 fair ride inspections, and returned over $2.8 million to consumers through mediations with businesses.

The Division of Food Safety monitors food from the point of manufacturing and distribution through wholesale and retail sales to ensure the public of safe, wholesome and properly represented food products.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

The Consumer Product Safety Commission provides consumer product recall information as part of the agency's mission to protect consumers and families from hazardous products.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection and information. Consumers who would like information about filing a complaint against a business or who believe fraud has taken place can visit us online at FloridaConsumerHelp.com or contact the department's consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) for Spanish speakers.