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

CYBER SAFETY TIPS FOR TRAVELERS

These days, no matter where you're headed, being continuously connected is part of the travel plan. As you embark on your next adventure, the National Cybersecurity Alliance urges travelers to stay cyber safe while away from home by following some simple practices to help keep your devices safe and your vacation plans from going awry.

1. **Set up the "find my phone" feature on your devices.** Before you head out on vacation, this setting will allow you to find, remotely wipe data and/or disable the device if it gets into the wrong hands.

2. **Think before you book.** When booking flights and hotels online, use caution to avoid falling victim to fake third-party booking companies. The best option to is to book through the official website of the airline or hotel. Stick to reputable booking websites and verify their credibility through reviews. Always double-check the website URL for authenticity. Be wary of deals that seem too good to be true!

3. **Get savvy about WiFi hotspots.** Do not transmit personal info or make purchases on unsecure networks. Instead, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

4. **Protect physical devices.** Ensure your devices are with you at all times. If you are staying in a hotel, the best thing to do is lock them in a safe or lock them in your luggage. Using your device at an airport or cafe? Don't leave it unattended with a stranger while you get up to use the restroom or order another latte. Keep your devices with you at all times. The phrase "stranger danger" also applies to cybersecurity.

5. **Actively manage location services.** Location tools come in handy while planning navigating a new place, but they can also expose your location - even through photos. Turn off location services when not in use.

Visit StaySafeOnline.org for more online safety tips from the National Cybersecurity Alliance.

P2P "ACCIDENTAL" PAYMENT SCAMS

Peer-to-peer (P2P) payment services offer instant transfers, which means you can send and receive money within minutes, regardless of where you are. P2P payment apps have made it easy to send money to friends and family without having to write a check or visit a bank or ATM, but using the apps is not completely risk free. Scammers have devised scams to take advantage of unsuspecting users.

One such scam involves an "accidental" transfer of funds. If you receive money through a P2P payment app from someone you don't know, you may assume it was sent by accident because someone mistyped a friend's username or email address. However, this may be an attempt to scam you out of your hard-earned money.

Here's how the scam works:

- The scammer creates a profile on a P2P payment app, links a stolen credit card number to the account, and uses the app to send payments to other users.
- The scammer then messages the recipient(s) through the app, claiming the payment was sent by mistake, and begging the recipient to pay the funds back.
- Before the recipient can return the funds, the scammer replaces the stolen card on the app with a personal card, to which the recipient's payment is applied.
- Later, the owner of the stolen card may dispute the fraudulent payment, causing the funds to be pulled from the recipient's account. In that case, the recipient becomes the victim, having already "returned" the funds to the attacker.

If you receive an "accidental" payment through your P2P app from someone you don't know:

1. Do not follow return payment instructions from a stranger.

2. Ask the sender to cancel the transaction immediately — in many cases, the sender can simply contact the app's customer support to cancel the transaction.

3. If the sender refuses to do so, contact the app's customer support yourself, explain the situation, and ask them to reverse the transaction.

Here are some additional steps you can take to protect yourself while using P2P payment apps:

- **Pay it safe:** Only send funds to those you know and trust. Most P2P apps don't allow you to cancel a transaction, treat payments like cash.
- **Take your time:** If someone is pushing you to act quickly with a P2P payment, it could be a red flag.
- **Use your security settings:** Enable settings within the P2P applications, such as multifactor authentication (also known as two-factor authentication).
- **Let your financial institution help:** Sign up to receive fraud alerts, and always contact your financial institution immediately if you suspect something is wrong.
- **Be aware of phishing:** Fraudsters might try to access your account by posing as your financial institution or a P2P company. If someone calls you unexpectedly and claims to be from your financial institution, it is best to hang up and call your financial institution at the number printed on your statement rather than the number that called you.
- **Use unique passwords:** Use different passwords for P2P apps and other sites, avoid sharing your passwords with others, and consider a password manager tool if you have trouble remembering passwords.

SUBSCRIPTIONS AND FREE TRIALS

Subscriptions aren't just for newspapers and magazines anymore. A subscription is simply an agreement to pay money to get a product or service regularly, and there are subscription offers out there to fill almost any want or need. You can subscribe to services that will deliver goods ranging from vitamins and beauty products to clothes and dog food right to your door.

Many subscription offers are tempting, especially if they offer a free trial period before you commit. One potential problem with free trials is that you may be required to provide your credit card information when you sign up for them. If you don't read the terms carefully, you may inadvertently agree to allow the company to start charging your card right away when the trial ends.

Before signing up for a free trial, be sure you understand the terms of the agreement. Take the following steps to protect yourself:

- Read all the details. Unless it is made clear to the contrary, you should assume that the business will start charging you when the free trial period is over.
- Look for pre-checked boxes. Some businesses use these hoping you won't notice that you're agreeing to be billed later. Uncheck the box if you don't agree with what it says.
- Find out when and how you must cancel before you sign up for the service. Businesses should make this easy for you. It's the law. If it's not clear to you how to cancel, walk away.
- Check to see if you can cancel online.
- Make a note on your calendar about the date of cancellation.
- Check reviews of the company to find out if they were cooperative with the cancellation process.

But what if you're receiving a product by subscription you never ordered? How do you stop it?

The Federal Trade Commission (FTC) has received complaints from folks who are being charged for subscriptions they don't want and never ordered. When contacted, some subscription services say that people must speak to a different company. People have also reported getting error messages when they try to cancel online.

The FTC offers the following steps to stop an unwanted subscription:

First, know that you never have to pay for something you didn't order. If you get it in the mail, you never have to return it. Unauthorized debiting is a crime if they get your billing info and start charging you.

Contact the company that runs the subscription you want to cancel. If the company has instructions on how to cancel, follow those. Keep a copy of your cancellation request, along with notes about any conversations you had and how and when you canceled.

Watch your bank or credit card statements. Check for charges on your debit or credit card after you canceled the subscription. If a company won't stop charging your account after you've tried to cancel a subscription, file a dispute (also called a "chargeback") with your credit or debit card.

- Online: Log onto your credit or debit card online account and go through the dispute process.
- By phone: Call the phone number on the back of your card and tell the company why you're filing a dispute.

Follow up with a letter to your credit or debit card company. Follow up in writing by sending a letter to the address listed for billing disputes or errors. Use this sample letter.

If you've been charged for a subscription you didn't agree to, report it to the FTC at ReportFraud.ftc.gov or file a complaint at FloridaConsumerHelp.com.

FRANKENSTEIN FRAUD

According to the Federal Trade Commission (FTC), over 85% of identity theft is synthetic, and experts have coined a term for this particular type of cybercrime – Frankenstein fraud.

Frankenstein fraud, or synthetic identity theft, happens when fraudsters steal and mix various peoples personally identifying information (PII) to create an identity of someone that doesn't exist. The key piece of PII used in the scheme is a Social Security number (SSN). The fraudsters will search for SSNs that either don't have an associated credit history or are unlikely to be actively monitored, i.e., numbers for children, recent immigrants, elderly individuals, incarcerated people, and deceased people.

Using the synthetic identity, fraudsters will apply for phone numbers; set up email, reward card, library card, and social media accounts; and take steps to put the identity into public databases used by financial institutions to verify identity information. Over a period of months or even years, fraudsters will nurture these synthetic identities while building a fraudulent credit profile through applications and inquiries and creating false credit reporting agency updates. Once they have obtained loans and credit cards with the synthetic identity, the fraudsters will max out those accounts and disappear with the money.

It would appear that the biggest victims of Frankenstein fraud are the financial institutions that provide the loans or credit, and they are, without a doubt, victims. However, of great concern are the children whose identities are compromised in the creation of a synthetic identity. The theft of their identity may remain unnoticed for years, and only be discover when they become credit-active adults.

The FTC recommends the following steps to protecting your identity:

- Read your credit card and bank statements carefully and often.
- Know your payment due dates. If a bill doesn't show up when expected, find out why.
- Shred any documents that include PII for you or your children.
- Delete personal information before disposing of a computer or cell phone.
- Review each of your three credit reports at least once a year.
- Request a credit freeze. Anyone can request a credit freeze, or security freeze, by contacting each of the three credit bureaus. You can also request a freeze for a child under 16, making it harder for someone to open new accounts in their name.

If you have been a victim of identity theft, visit IdentityTheft.gov, the federal government's one-stop resource to help you report and recover from identity theft.

TOP TEXT SCAMS OF 2022

By Emma Fletcher, Federal Trade Commission

Texting is cheap and easy, and scammers are counting on the ding of an incoming text being hard to ignore. In 2022, they were right to the tune of $330 million in losses to text scams, as reported to the FTC's Consumer Sentinel Network, with a median reported loss of $1,000. That's more than double the 2021 reported losses and nearly five times what people reported in 2019. In fact, reports about text scams spiked in the first six months of the COVID-19 pandemic and have never returned to pre-pandemic levels.

But why do they work? Scammers use the speed of text communication to their advantage: they hope you won't slow down and think over what's in the message. Some messages promise a good thing – a gift, a package, or even a job. Others try to make you panic, thinking someone's in your accounts. These are all lies and ways to take your money and personal information.

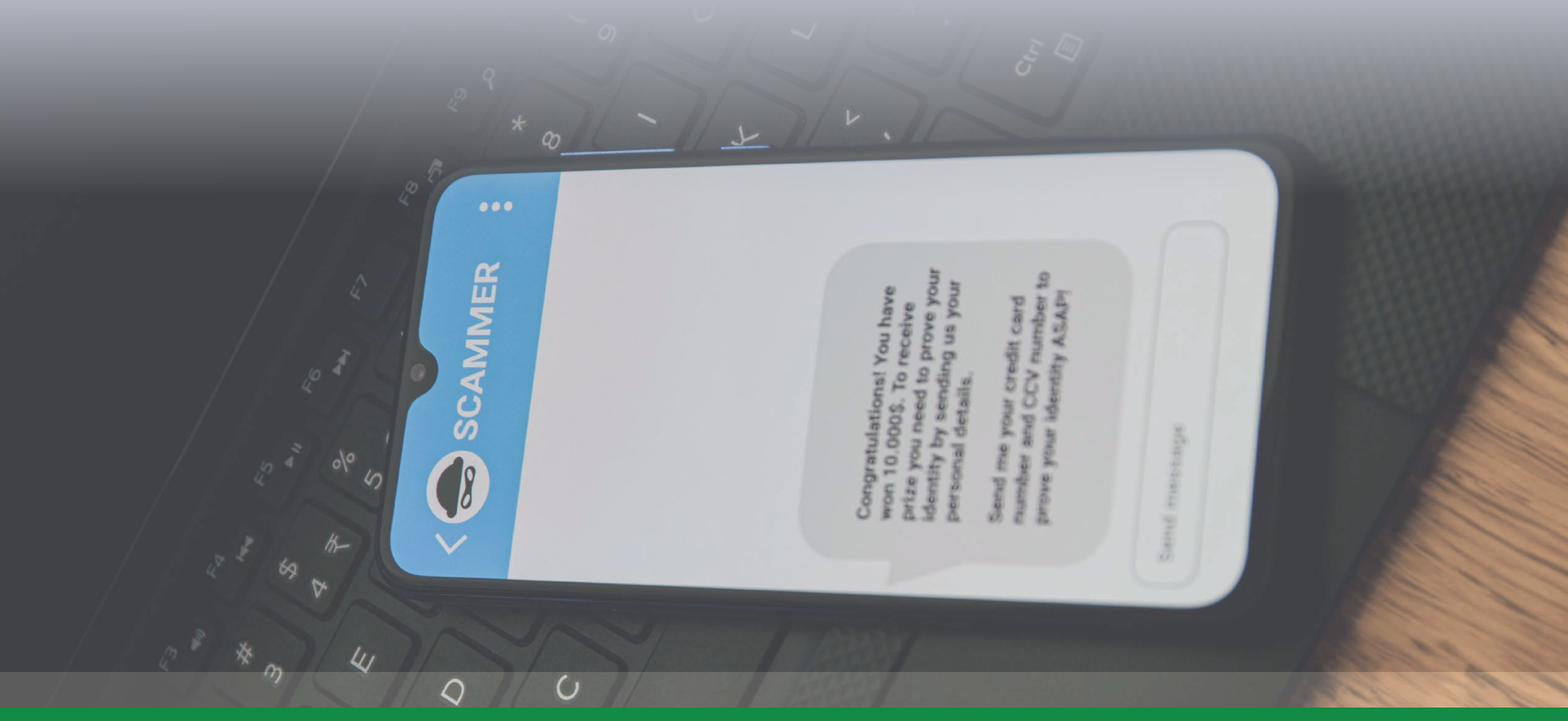
While there are countless varieties of text scams, the top five described below account for over 40% of randomly sampled text frauds reported in 2022. All five have one thing in common – they often work by impersonating well-known businesses.

1) Copycat bank fraud prevention alerts

Reports about texts impersonating banks are up nearly twentyfold since 2019. You might get a fake number to call about supposed suspicious activity. Or they might say to reply "yes or no" to verify a large transaction (that you didn't make). If you reply, you'll get a call from the (fake) fraud department. People say they thought the bank was helping them get their money back. Instead, money was transferred out of their account. This scam's median reported loss was a whopping $3,000 last year. Worse still, many people report giving their Social Security number and other personal information to scammers, leading to possible identity theft.

2) Bogus "little gifts" that can cost you

A text about a free gift, reward, or prize may look like it came from a company you know – say, your cell phone company or a big retailer. But everything about this is fake. If you click the link and pay a small "shipping fee," you just gave your credit card number to a scammer. Reports tell us fraudulent charges soon follow.



3) Fake package delivery problems

Expecting a package? There's a text scam for you. Texts pretending to be from the U.S. Postal Service, FedEx, and UPS say there's a problem with a delivery. They link to a website that looks real – but isn't. If you paid a small "redelivery fee," which many people reported, that was a trick to get your credit card number. People also reported giving these scammers their personal information, including Social Security numbers.

4) Phony job offers

Promises of easy money for mystery shopping at well-known stores like Whole Foods and Walmart are an old scammer favorite. Reports about bogus offers to make money driving around with your car wrapped in ads are also common. Reports show job scammers also target people who post their resumes to employment websites like Indeed. In most of these reports, scammers use checks that seem to "clear" but turn out to be fake to trick people into sending them money.

5) Not-really-from-Amazon security alerts

Like fake bank texts, texts from someone who says they're "Amazon" look like automated fraud prevention messages. Often, they ask you to verify a big-ticket order you didn't make. If you call the number in the text, you get a phony Amazon rep who offers to "fix" your account. People often report giving the rep remote access to their phone so they can get things fixed and get their refund.[9] But then the rep says a couple of zeros were accidently added to the refund, so they need you to return that money to them – often by buying gift cards and giving the cards' PIN numbers.

In all these cases, reporting can help stop scam text messages:

- Forward it to 7726 (SPAM). This helps your wireless provider spot and block similar messages.
- Report it on either the Apple iMessages app or Google's Messages app for Android users.
- Report it to the FTC at ReportFraud.ftc.gov.

How can you avoid text scams?

- **Never click on links or respond to unexpected texts.** If you think it might be legit, contact the company using a phone number or website you know is real. Don't use the information in the text message.
- **Filter unwanted texts before they reach you.** There are a few ways to block unwanted texts.

To learn more about how to spot and avoid scams – and how to recover money if you've paid a scammer – visit ftc.gov/scams. Learn more about text scams at ftc.gov/textscams.

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.

Food Recalls

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.

Consumer Product Recalls

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.