FLORIDA CONSUMER
NEWSLETTER
January 2025
A publication of the Florida Department of Agriculture and Consumer Services

START OF TAX SEASON

IRS Form W-2, also known as a "Wage and Tax Statement," signals the beginning of tax season and is the form most people care about when preparing to file their federal taxes. The form shows the amount of money you earned and the amount of taxes withheld from your paychecks, as well as benefits provided during the previous year and how much you contributed to your retirement plan during the year. Information from Form W-2 is used when you file your personal tax returns – both federal and state – with the IRS and your state's tax agency and in calculating social security and Medicare benefits.

Employers are required to provide employees with a copy of Form W-2 by January 31 each year. These forms can be sent in either paper or digital form and are considered on time if they are properly addressed and mailed on or before January 31.

Identity theft is a real concern when filing taxes. Taxpayers who file via mobile, tablets, and apps using shared wireless networks are at greater risk of having their tax identity compromised. Protecting personal information and Social Security numbers year-round is the most important step in safeguarding an individual's identity. Aside from that, filing a tax return as early as possible is the next best thing you can do to prevent tax-related identity theft.

The Internal Revenue Service does not verify the validity of individual tax forms. The agency only becomes aware of issues when two returns are filed using the same Social Security number. If an identity thief has the right information, they can file a fraudulent tax return as early as January 20th and beat a legitimate taxpayer to their refund.

The Federal Trade Commission recommends the following steps to help prevent tax-related identity theft:

- Use a secure Internet connection if you file electronically, or if you are submitting a paper copy, mail your tax return directly from the post office.
- Shred copies of your tax return, drafts, or calculation sheets you no longer need.
- Respond to all mail from the IRS as soon as possible.
- Don't give out your Social Security number unless necessary.
- Research a tax preparer thoroughly before you hand over personal information.
- Check your credit report at least once a year for free to make sure no other accounts have been opened in your name.

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
    - o www.Equifax.com 1-800-525-6285
    - o www.Experian.com 1-888-397-3742
    - o www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves.

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist

.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

AVOID A FLOOD-DAMAGED USED CAR

CARFAX, a company that provides vehicle history reports for cars and trucks in the United States, has estimated that 347,000 cars suffered flood damage during the 2024 hurricane season. Approximately 120,000 vehicles in Florida were damaged during Hurricane Milton, and another 138,000 vehicles were impacted by Hurricane Helene across several states. While Hurricane Debby caused widespread flooding in the Big Bend regions, specific date on the number of damaged cars from that storm is not available.

Flooded cars are generally issued a new title called a "salvage title." This occurs when the vehicle has been deemed a total loss by an insurance company due to significant damage and the cost to repair it will exceed its market value. A salvage title essentially marks a vehicle as severely damaged and not legally drivable unless rebuilt and inspected to meet state standards.

Unscrupulous sellers may try to hide a vehicle's true history and defraud buyers by "title washing." This is the illegal practice of removing information, like flood damage, from a car title to make the vehicle easier to sell by presenting a "clean" title. Often these vehicles are transported out of the flood area to places where buyers may be less aware of the warning signs of flood damage.

Buyers may not know a car is damaged unless they look at it closely or have it inspected. The Federal Trade Commission recommends taking these steps when shopping for a used vehicle:

Check for signs and smells of flood damage. Is there mud or sand under the seats or dashboard? Is there rust around the doors? Is the carpet loose, stained, or mismatched? Do you smell mold or decay — or an odor of strong cleaning products — in the car or trunk?

Check for a history of flood damage. The National Insurance Crime Bureau's (NCIB) free database will show if a car was flood-damaged, stolen but not recovered, or otherwise declared as salvaged — but only if the car was insured when it was damaged.

Get a vehicle history report. Start at vehiclehistory.gov to get free information about a vehicle's title, most recent odometer reading, and condition. For a fee, you can get other reports with additional information, like accident and repair history. The FTC doesn't endorse any specific services. Learn more at ftc.gov/usedcars.

Get help from an independent mechanic. A mechanic can inspect the car for water damage that can slowly destroy mechanical and electrical systems and cause rust and corrosion.

Report fraud. If you suspect a dealer is knowingly selling a storm-damaged car or a salvaged vehicle as a good-condition used car, contact the NICB. Also tell the FTC at ReportFraud.ftc.gov and your state attorney general.

TASK SCAMS

By Jim Kreidler, Consumer Education Specialist, FTC

Have you been getting unexpected messages about online work? The FTC's new Data Spotlight highlights a big increase in the number of people reporting gamified job scams, or "task scams." Read on to learn what they are and how to avoid them.

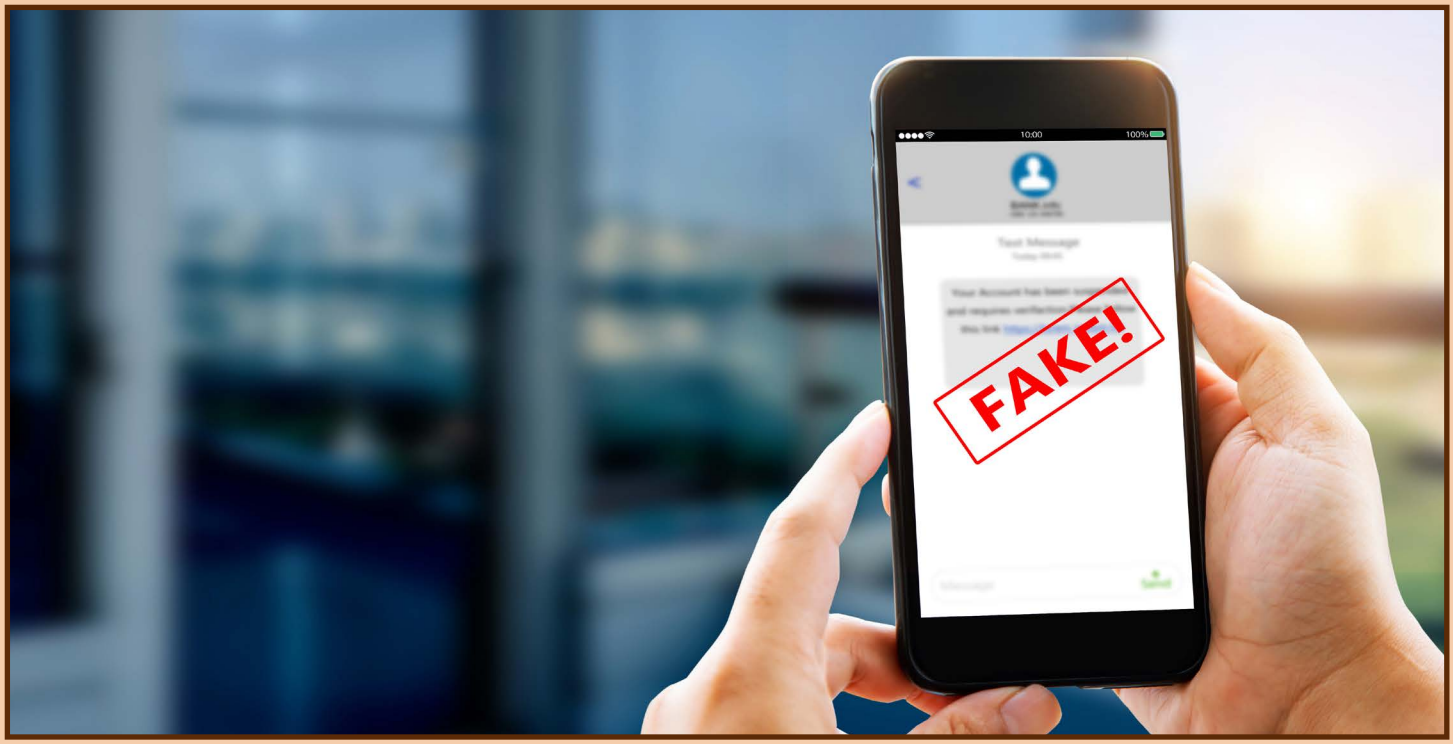
In a task scam, scammers ask you to do simple, repetitive tasks, such as liking videos or rating product images online. The supposed "job" is to complete tasks in an app or online platform for which you'll "earn money" from a "commission" on each click. But those promises are fake: there aren't any commissions, and nobody but the scammers make any money.

Task scams usually start with an unexpected text offering online work. They say you can "make good money" by "product boosting" or doing "optimization tasks" online. Once you complete each task, you'll see an ever-increasing tally of supposed earnings in the app. (They're fake.) At some point, the app or online platform will ask you to deposit your own money — usually in crypto — to complete your next set of tasks and to get your supposed (fake) earnings out of the app. But if you make the deposit, not only is your real money gone, you'll never get those fake earnings.

To spot and avoid task scams:

- Ignore generic and unexpected texts or WhatsApp messages about jobs. Real employers will never contact you that way.
- Never pay anyone to get paid, or to get a job. That's a sure sign of a scam.
- Don't trust anyone who says they'll pay you to rate or like things online. That's illegal and no honest company will do it.

Learn more about spotting and avoiding scams at ftc.gov/scams and report scams to the FTC at ReportFraud.ftc.gov.



HOSPICE FRAUD

By Kira Krown, Consumer Education Specialist, FTC

Did someone reach out and offer free, in-home perks like cooking and cleaning in exchange for your Medicare number? Don't give it. That could be a scammer trying to commit hospice fraud.

Scammers are targeting older adults — with calls, texts, emails, fake ads, and even door-to-door visits — claiming they'll set you up with services like free cooking, cleaning, and home health care. What they likely won't tell you is how: They want to commit fraud by signing you up for Medicare hospice — that's right, hospice — care. Then, they can bill Medicare for all kinds of services in your name.

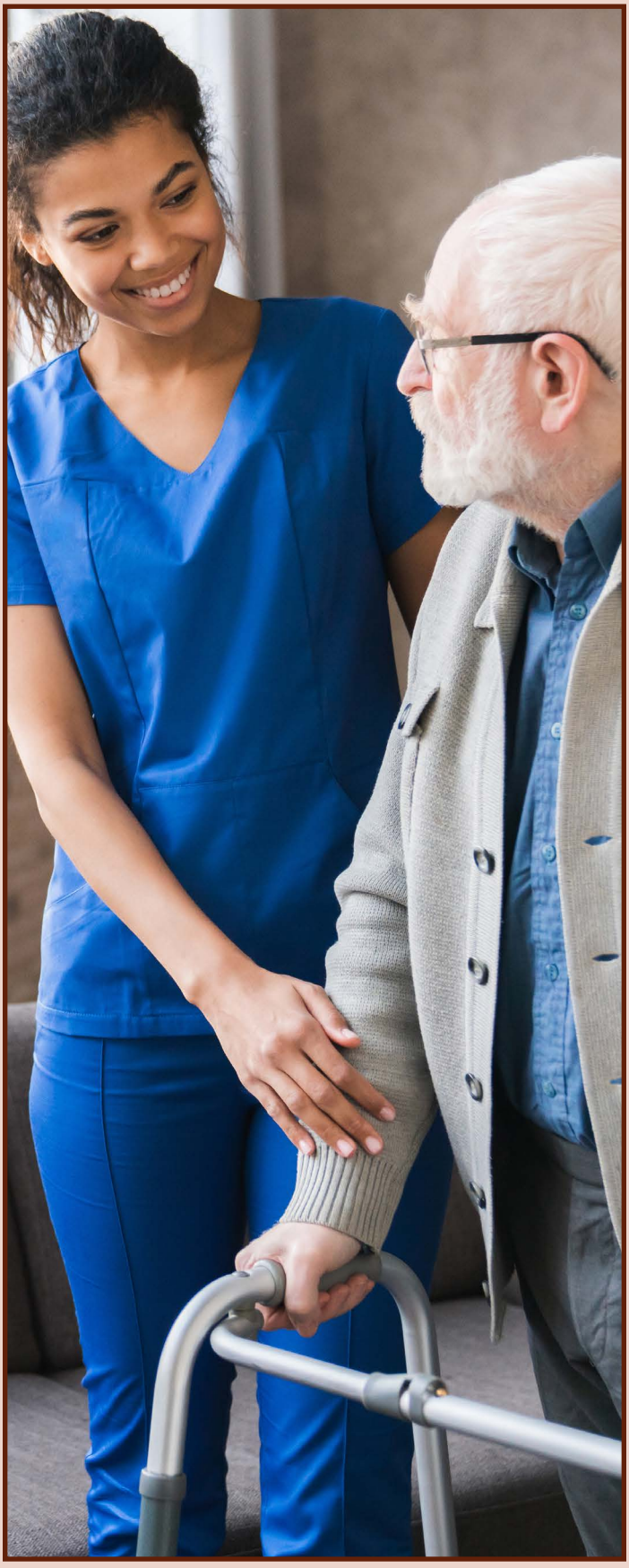
Here's what to know: Hospice care is a specialized service, often done at home, for people with a terminal illness approaching the end of life. Only your doctor can certify that you're eligible for hospice (meaning your life expectancy is 6 months or less). If you're signed up for hospice and don't need it, this could affect your Medicare coverage in the future. Anyone who tells you differently is a scammer.

Here are some ways to avoid hospice scams:

- Never give your Medicare number to someone offering "free" services like housekeeping or cooking. Medicare doesn't offer free services like that.
- Never agree to sign up for hospice care in exchange for perks or gifts like money, gift cards, or groceries.
- Know that Medicare will never come to your home to sign you up for services. If someone comes to your door, says they're from Medicare, and tries to get you to sign up for services, they're lying. Don't give them any information.

If you think you've spotted or experienced hospice fraud, report it as soon as possible. Call 1-800-MEDICARE or reach out to your local Senior Medicare Patrol for help.

Learn more at Medicare.gov/fraud.



PHISHING SCAMS

By Ari Lazarus, Consumer Education Specialist, FTC

Scammers love a good disguise. One day they show up texting you about a delivery you missed, the next they say you need to sort an issue with your Netflix account. Here's how to avoid these phishing scams.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. Maybe it's an unexpected email or text message pretending to be from a company you know or trust, like a utility company asking you to make a payment. Or maybe it's an unexpected party invitation that looks like it's from a friend or family member.

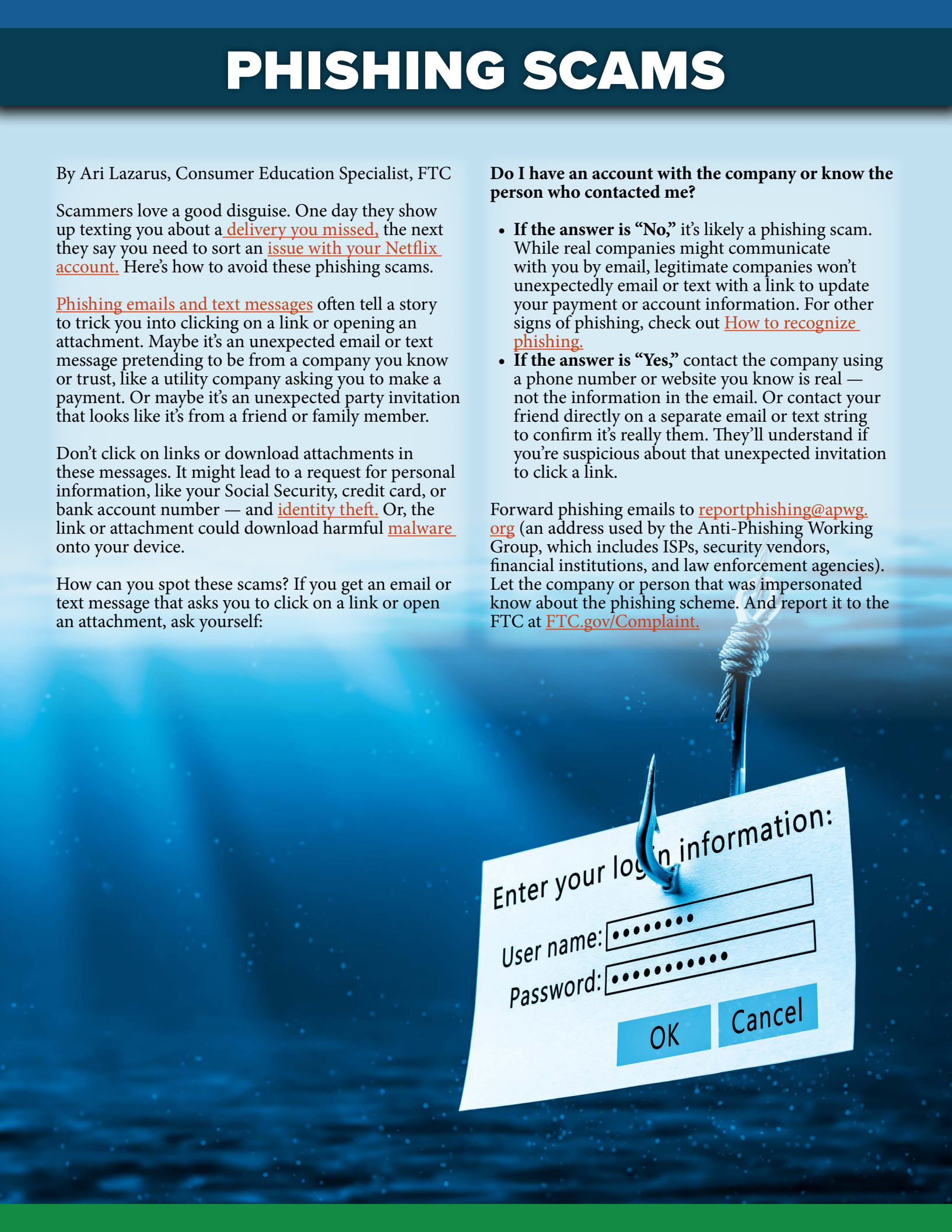
Don't click on links or download attachments in these messages. It might lead to a request for personal information, like your Social Security, credit card, or bank account number — and identity theft. Or, the link or attachment could download harmful malware onto your device.

How can you spot these scams? If you get an email or text message that asks you to click on a link or open an attachment, ask yourself:

Do I have an account with the company or know the person who contacted me?

- **If the answer is "No,"** it's likely a phishing scam. While real companies might communicate with you by email, legitimate companies won't unexpectedly email or text with a link to update your payment or account information. For other signs of phishing, check out How to recognize phishing.
- **If the answer is "Yes,"** contact the company using a phone number or website you know is real — not the information in the email. Or contact your friend directly on a separate email or text string to confirm it's really them. They'll understand if you're suspicious about that unexpected invitation to click a link.

Forward phishing emails to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme. And report it to the FTC at FTC.gov/Complaint.



HACKED EMAIL OR SOCIAL MEDIA

By Alvaro Puig, Consumer Education Specialist, FTC

Hackers target your email and social media accounts to steal your personal information. Like your username and password, bank or credit card account numbers, or Social Security number. If they get it, they use it to commit identity theft, spread malware, or scam other people. So, what are signs that someone hacked your account, and how can you recover a stolen account?

Here are some things that might tip you off to a problem:

- You get a notification that your email address or phone number changed. Or that your password was reset. But you didn't make those changes.
- You get a message that someone tried to log in, or did log in, and it wasn't you.
- You can't log in to your account.

If you can't log in to your account, follow the provider's account recovery instructions. Here are links to some of them.

Facebook	Microsoft	WhatsApp
Google	Pinterest	X
Instagram	Reddit	Yahoo
Linkedin	Snapchat	YouTube

If you get a notification about activity you don't recognize, and you can log in, here's what to do:

Change your account password. Create a unique and strong password that is hard to guess. Aim for 12 to 15 characters. Or use a passphrase — a series of words separated by spaces. Then sign out of that account on all devices. That way anyone who's logged in to your account on another device will get kicked out.

Secure your account. If the account offers two-factor authentication (2FA), turn it on to add an extra layer of security. That way, a hacker with your password can't log in to your account without a second authentication factor. Like a verification code you get by text or email, or from an authenticator app.

Update your account recovery information. Account recovery information helps you get back into your account if you're locked out, forgot your password, or if someone else is using it. Check your account recovery information and make sure the email address and phone number listed are correct.

Check for signs that someone had access to your account. Check if there are auto-forwarding rules in your email account that you didn't set up. Hackers might create these rules to forward your emails to another address. Check your social media for messages the hacker posted or sent, or for new friends you don't recognize.

If you believe someone stole your personal information, go to IdentityTheft.gov to report it and get a personalized recovery plan.

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.