Protect yourself from Scams

October 2022

Protect yourself from digital scams

Victims of Internet-related crimes reported losing $4.1 billion in 2020, according to the Federal Bureau of Investigation's Internet Crime Complaint Center. Illinois ranked sixth, with more than $150 million in reported losses. This fact sheet will give you information about typical scams and how to protect yourself, as well as tips on what to do if you fall victim to a scam.

Summary of typical scams

Utility imposter scams: Fraudsters call customers and threaten them with shut-off if they don't make an immediate payment. Utilities don't ask for payment via money cards or cash apps.

General imposter scams: Scam artists use texts, emails, calls or a pop-up to claim they represent the Internal Revenue Service (IRS), Social Security Administration, tech support from an established company or some other official source. That's not how those places reach out to you. Never provide personal information via text, email or over the phone.

Electric scams. The robocall promises a refund or discount on your power bill and asks you to press 1. That's when a salesman comes on and tries to switch you to an alternative supplier that could easily charge you much more than your utility rate.

Online shopping scams. Beware of deals that seem too good to be true. If you shop online, avoid clicking on advertisements and go directly to the retailer's website.

Sweepstakes scams. If a pop-up says you've won a prize from a sweepstakes you don't remember entering, it's most likely a scam. Don't click on links or call numbers displayed and don't provide personal or financial details. If a sponsor is listed, contact them at a number you find yourself to confirm whether it's legitimate.

Protect yourself from potential scams

- Do not click on suspicious links or provide personal details. If in doubt, reach out to that agency or company on your own through a legitimate phone number or website that you find yourself. Don't trust any number or URL that the potential scammer provides.
- Delete suspicious emails and texts. (While an email or text may look official, a closer inspection of the message may reveal spelling errors and bad grammar. If you ever get an official-looking text or email with a disturbing warning, don't do anything rash. Again, contact the company/agency yourself.)

- Hang up on calls that ask you to provide personal information, such as your Social Security Number or bank account number.
- Keep your software up to date. Most devices can be set to update automatically when new software versions are released.
- Back up your data. You can copy your computer files to an external hard drive or cloud storage. It's good practice to back up the data on your phone, too.
- Set up two-factor authentication. Some devices offer extra security by requiring two or more credentials to log in to your account. This way, if scammers get your password, your device is still protected.

What To Do if You Were Scammed

If You Paid a Scammer…

- **Credit or Debit Card:** Contact your bank or credit card company to tell them there was a fraudulent charge. Ask them to reverse the transaction and give you your money back.
- **Bank Transfer:** Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.
- **Gift card:** Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.
- **Wire transfer:** Contact the bank or wire transfer company to tell them there was a fraudulent charge. Ask them to reverse the transfer and give you your money back.
- **Money Transfer App:** Report the activity to the app's company and ask to reverse the payment.
- **Cryptocurrency:** While typically not reversible, it doesn't hurt to ask the transfer company if there's a way to reverse the transfer.
- **Cash:** If you sent cash via a delivery service, contact them as soon as possible. The U.S.Postal Inspection Service can attempt to intercept the package if sent by mail. Contact them at 877-876-2455.

What to do if you are scammed (Continued)

If You Gave a Scammer Your Personal Information

- Go to **IdentityTheft.gov** to see what steps to take, including how to monitor your credit.
- Create a new, strong password if they have access to your accounts. If you use the same password anywhere else, change it there, too. (See our password tips below.)

If a Scammer Has Access to Your Computer or Phone

- Update your computer's security software, run a scan and delete anything identified as a problem.
- Contact your service provider immediately if the scammer has control of your cellphone number and/or service account.

Report a Scam to the Federal Trade Commission

When you report a scam, the FTC can use the information to build cases against scammers, spot trends, educate the public, and share data about what is happening in your community. If you experienced a scam or even spotted one, report it to the FTC at **ReportFraud.ftc.gov**.

Report a Scam to the Illinois Attorney General

The Illinois Attorney General's office has fraud protection resources at **IllinoisAttorneyGeneral.gov/Consumers**. Here are their fraud hotlines:

Chicago
1-800-386-5438
1-800-964-3013 (TTY)

Springfield
1-800-243-0618
1-877-844-5461 (TTY)

Carbondale
1-800-243-0607
1-877-675-9339 (TTY)

Spanish Language Toll-Free Hotline: 1-866-310-8398

Helpful Resources

- **CitizensUtilityBoard.org:** Helpful consumer tips, including CUB's Guide to Fighting Robocalls
- **IdentityTheft.gov:** A one-stop resource for victims of identify theft.
- **FBI.gov:** Search for "scams and safety" for tips on the Federal Bureau of Investigation (FBI) website.
- **DoNotCall.gov:** The FTC's Do Not Call Registry. Scammers get around the Federal Trade Commission's Do Not Call Registry, but it's still a good idea to join. It's free, and you will get fewer robocalls from companies that follow the law—then you know a sales call is likely from a scammer.

Tips on Creating Strong Passwords

- Avoid common words and numbers connected to you—your name, birthday and phone number—as well as "1234" and "qwerty."
- The FTC recommends a password of at least 12 characters. Mix uppercase and lowercase letters, numbers, and symbols.
- Consider using a passphrase--not a famous saying ("To be or not to be), but something unique to you, such as "Uncle George is my #1 relative."
- Don't email or text passwords, or say them over the phone.
- Avoid storing passwords on a computer or device protected by those passwords. Write them down and keep them in a secure place. Or you can use a password manager application. These apps generate strong passwords for all your accounts and "encrypt" them, making them unreadable to anyone else. You can find a reputable password manager by searching independent review sites and talking to friends and family.