HOW TO OUTSMART

IDENTITY THIEVES

Rural Mutual and CyberScout have teamed up to teach you what you need to know to protect yourself from online scammers. Here's a list of today's top cyber scams to be aware of and watch out for – and ways to avoid falling victim to them. Download and print this guide for a handy reference.

CYBERSCOUT
A Sontiq™ Brand

Rural Mutual Insurance Company

THE SCAM:

COVID-19 VACCINATION CARD SELFIES

Those seemingly innocent proof of vaccination card selfies seen everywhere on social media make for an immediate windfall for scammers. Since the cards display people's full names, birthdates and information on where they got their shots, thieves can obtain the data they need to break into bank accounts and open credit cards and loans in your name.

OUTSMART THE THIEF

- Stick with a generic "I got vaccinated!" sticker selfie.
- Use the "Got My Vaccine" profile picture frame available on social channels.
- Secure your social media settings and change passwords at least quarterly.
- Put your vaccination card in a safe and secure location like a file cabinet or bank safety deposit box.

THE SCAM:

LET'S GO PHISHING

Phishing schemes, which use phony email addresses and phone numbers to convince people to turn over confidential information, are extremely common with over 200,000 phishing sites identified by the APWG Phishing Report. CyberScout reports that voice phishing – commonly known as vishing – is growing in popularity as fraudsters attempt to collect personal data from vulnerable people.

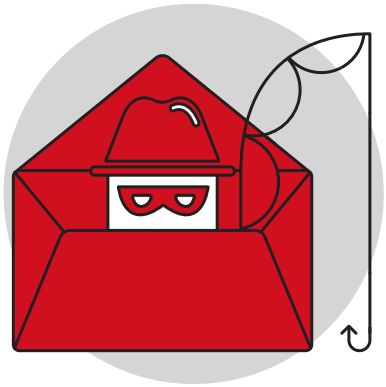
There's also "Zoom phishing," in which con artists set up fake Zoom sites and send out emails falsely warning people that their Zoom account is suspended or that they missed a meeting. Clicking on these convincing links allows malicious software to be installed onto your computer, providing thieves with access to your personal data.

OUTSMART THE THIEF

- Never open or click on unsolicited emails, text messages, social media messages or phone messages. If you don't recognize the sender, delete the message immediately and report it as spam.
- If someone says there's a problem with your Zoom (or any other) account, visit the real website at Zoom.us and reach out to the official customer support team.

CYBERSCOUT®
A Sontiq™ Brand

Rural Mutual Insurance Company



THE SCAM:

SMISHING–
SCAM BY TEXT

As if phishing weren't bad enough, now thieves are upping the ante with fake text messages to cell phones containing "urgent" messages about credit cards or bank accounts, contest prize notifications, fake survey links and messages from trusted brands. All these scams ask you to verify your identify or provide sensitive personal information.

OUTSMART THE THIEF

- Look for noticeable bad grammar and spelling errors.
- Links provided in messages are slightly off (e.g., ama.zon.com vs amazon.com).
- Verify all messages you receive, even if it's from a company you buy from often to ensure that the contact is genuine. Just like URLs and emails, phone numbers can be faked, so it's important to double check.

CYBERSCOUT®
A Sontiq™ Brand

Rural Mutual Insurance Company

THE SCAM:

PEER-TO-PEER PAYMENT APPS

Payment apps like Venmo, PayPal, Zelle and Google Pay help users quickly transfer money. However, like most digital services, these apps have malicious users who are up to no good. Look out for application fraud with strangers signing up for apps pretending to be you and pulling money from your account. The "accidental transfer of funds" scam has hackers using stolen bank cards to transfer money to unsuspecting users. If you send the money back to the scammer to refund them, they will delete the stolen credit card from their account and add their own card in its place. Then, the money you send goes to their personal card. Eventually, the stolen funds will be removed from your account, and you will be out that money.

OUTSMART THE THIEF

- Carefully review all payment requests before hitting accept.
- Ignore requests to return accidental deposits.
- Disable incoming requests on your app and only use the app to send money.
- Report any incidents immediately to the app's support team.

THE SCAM:

IRS CALLS FOR YOUR SOCIAL SECURITY NUMBER

Scammers call, email, text or reach out via social media pretending to be from the Internal Revenue Service. They request your social security number or other personal information related to taxes, stimulus checks or another claim that you owe the IRS money.

OUTSMART THE THIEF

- Hang up on any phone calls and delete messages that ask for your social security number.
- Call an authorized IRS representative to verify whether the agency is trying to reach you. The IRS typically initiates contact with taxpayers through U.S. mail, so chances are, a phone call is not legitimate.

THE SCAM:

BEWARE OF RANSOMWARE

Ransomware is malicious software that infects a computer and restricts a user's access until a ransom has been paid. This scam has exploded on the scene and impacts both individuals and businesses. For individuals, the requested amount usually ranges between $200 and $400 and must be paid in a virtual currency like Bitcoin. For businesses, especially healthcare organizations, the impact can be disastrous with ransoms running in the millions.

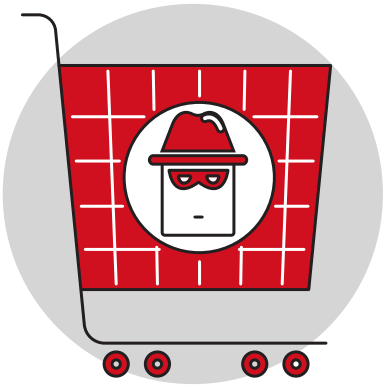
OUTSMART THE THIEF

To avoid ransomware:

- Make sure you have updated security systems, including anti-virus software, on your devices.
- Send incident reports when your system requests them.
- Don't click unsolicited web links in emails.

If you are a ransomware victim:

- Immediately disconnect from networks and external devices (e.g., phones, cameras and USB drives).
- Don't pay the ransom as this doesn't guarantee the release of your data.
- Contact your local FBI field office to request assistance and submit a tip online.



THE SCAM:

ONLINE SHOPPING FRAUD

Who doesn't love a great online sale? Along with these deals come devious online thieves who have devised limitless ways to rip innocent customers off, especially during the holiday season, when 84% of Americans shop online, according to CyberScout. In addition to phishing emails, online shoppers need to be aware of fake e-retailers with bargain basement discounts. Some deliver shoddy merchandise while others don't deliver anything at all. Some will even send email coupons with malware that infects your computer and steals your data.

OUTSMART THE THIEF

- Look for website URLs and links with extra words or characters or that are poorly written.
- If the customer service representative uses a Yahoo or Gmail account instead of a corporate address, it's likely fake.
- Use trusted retail websites instead of shopping with a search engine.
- Comparison shop and research any unknown brands before making an online purchase.

CYBERSCOUT®
A Sontiq™ Brand

Rural Mutual Insurance Company

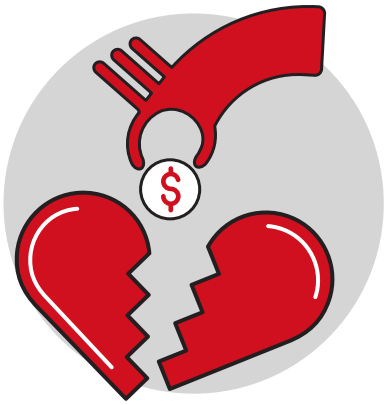
THE SCAM:

GET-RICH-QUICK SCHEMES

High school and college students are the main targets for schemes that promise financial aid or fake scholarships. Faux arts and literature contests that lure work submissions for a fee are also common, but students end up never seeing their work published. Acting and modeling gig scams that claim “talent scouts” are searching for the next star require upfront payment for headshots or acting lessons.

OUTSMART THE THIEF

- Search reputable art and literature publications and websites for genuine opportunities to showcase your work.
- Walk away from any scholarship, job or contest that requires you to pay upfront.



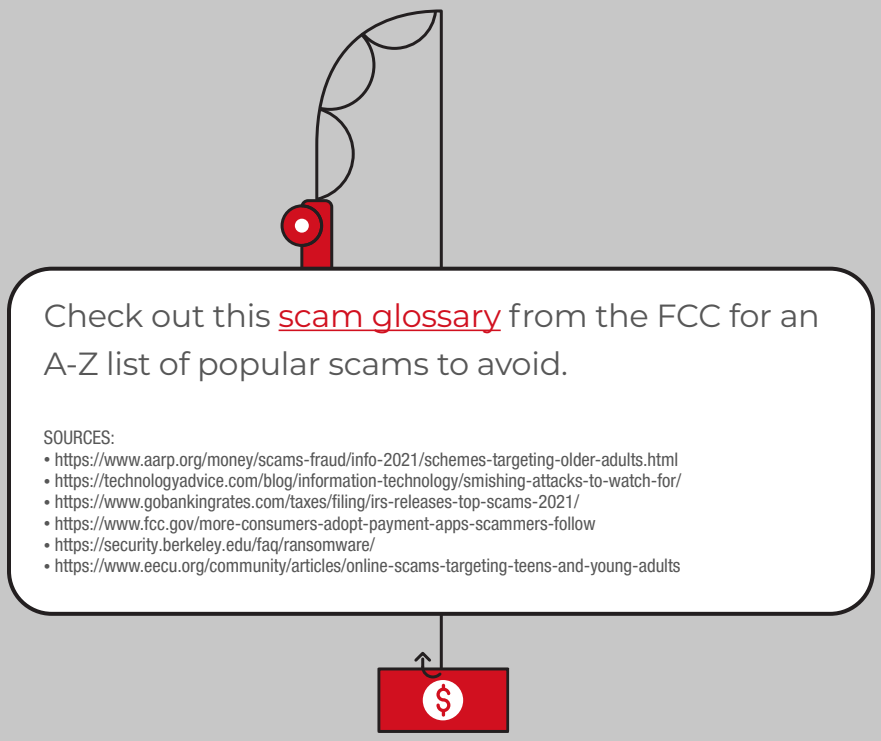
THE SCAM:

ONLINE ROMANCE GONE WRONG

Nice try, Nigerian prince. We're on to your game! Some scams have become easier to spot with time. But other online schemes, like those involving online dating, are harder to spot and can cause emotional damage and financial losses exceeding $230 million annually. These Romeo scammers troll online dating sites and chat rooms looking for vulnerable individuals. They build relationships and gain their "significant other's" trust over time. The fraud typically begins with money requests for travel or help with medical care.

OUTSMART THE THIEF

- Always verify people's identities by cross-checking other sites like LinkedIn, Facebook, etc.
- Beware of anyone who professes love too quickly or claims to be from the U.S. but is currently "overseas" for business or military service.
- Watch for anyone who tries to lure you off a dating site to communicate via phone or email – or worse yet, in-person. Instead, set up an alternative email address or an instant messaging app that isn't connected to any personal information.



Check out this scam glossary from the FCC for an A-Z list of popular scams to avoid.

SOURCES:

- https://www.aarp.org/money/scams-fraud/info-2021/schemes-targeting-older-adults.html
- https://technologyadvice.com/blog/information-technology/smishing-attacks-to-watch-for/
- https://www.gobankingrates.com/taxes/filing/irs-releases-top-scams-2021/
- https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow
- https://security.berkeley.edu/faq/ransomware/
- https://www.eecu.org/community/articles/online-scams-targeting-teens-and-young-adults

CYBERSCOUT
A Sontiq™ Brand

Rural Mutual Insurance Company