SecurityAwarenessNews

the security awareness newsletter for security aware people

Taking Security Personally

Scam Alert: Stay Aware of These Common Cons

Security Tips To Share With Friends and Family

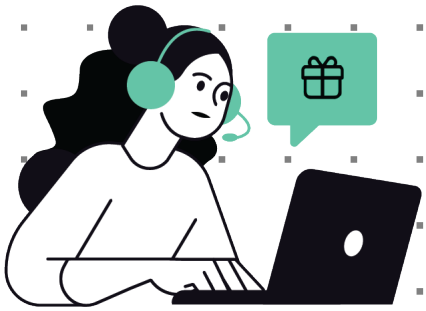
Staying Safe on Social Media

Scam Alert:
Stay Aware of These Common Cons

Security requires a proactive mindset, both at work and at home. While many attackers hope for a big payday by targeting large organizations, they'll also gladly scam regular people out of money or personal information. Let's review a few common ways they do this.

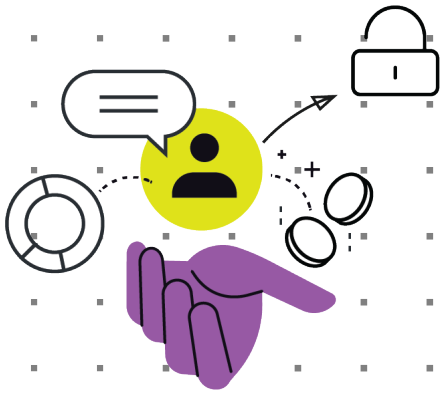
The Alarmist

This common scam arrives as an email that looks like it's from a real organization (a bank, a popular online store, a social media site). The message claims your account has been suspended due to suspicious activity. It requires that you open a link and update your username and password immediately, or the account will be permanently closed.



The Caller Who Demands Payment by Gift Cards

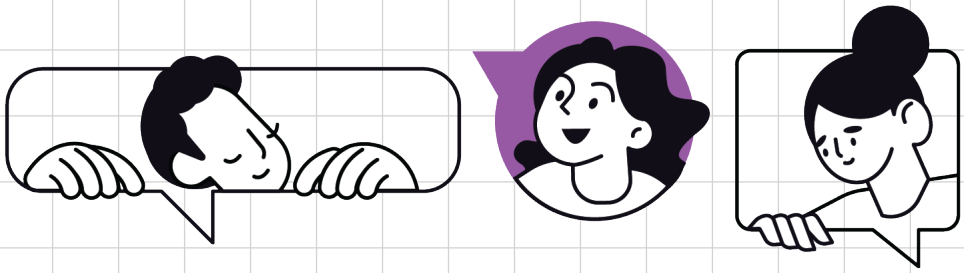
Imagine receiving an urgent phone call from someone who claims to be from a utility company. They tell you that your payment is overdue and threaten to cut off your power if you don't make an immediate payment. However, instead of using a traditional payment method, they ask you to purchase gift cards (for stores, online services, etc.) and read the card numbers to them over the phone.



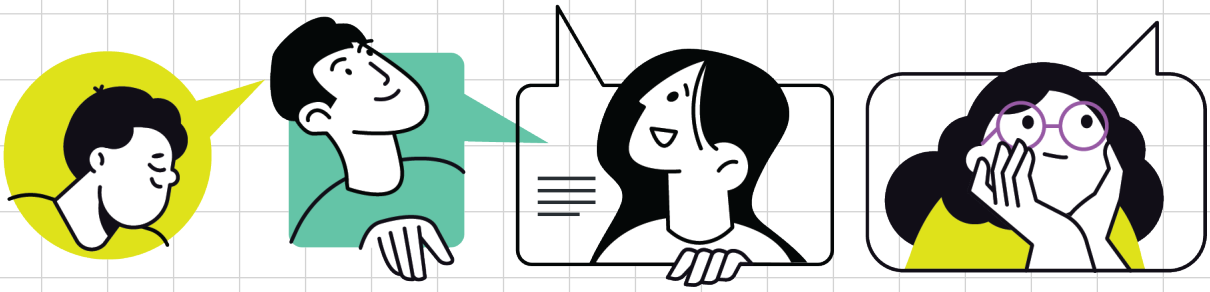
The Extortionist

Fear is a powerful ingredient in extortion scams. They typically involve an email with a threatening subject line, such as "I saw what you did." The messenger claims they hacked your computer and recorded your screen or accessed your webcam. They then threaten to send the video to all of your contacts unless you immediately pay the scammer.

The goal of most of these scams is to steal your money or your personal information. You can avoid them by slowing down, thinking critically, and never opening suspicious links or sending money to strangers.



Security Tips To Share With Friends and Family



Many of the principles that protect your organization from threats are the same ones that can protect your loved ones from scams. Here are some simple but powerful tips you can share to help keep everyone safe.

Scams are common, but there are almost always warning signs.

Scammers try to create situations that prevent you from thinking clearly and logically. They do this by targeting human emotions and manipulating them, leading people to make poor security decisions. But you can avoid this by staying alert for warning signs, such as urgent requests, threatening language, and unrealistic promises or scenarios.

Give your passwords a security boost.

How many passwords do you have? Most people have dozens. What's the best way to remember them all? The answer is to not even try. Instead, consider using a password manager, which is software that generates complex passwords and stores them securely for you. All you need to remember is one main password to unlock the manager.

If something is too good to be true, then it's likely fake.

Scammers often lure people in with promises of easy money. Be skeptical of any offer that promises a large reward for little or no effort. This includes:

- "Investment opportunities" that guarantee huge, risk-free returns
- Unbelievable discounts on valuable goods, like high-end electronics or luxury travel packages
- Notifications that you have inherited money from a relative you've never heard of

Keep your software and devices updated.

Developers often release updates designed to address critical security issues. Failing to install these updates could leave your devices vulnerable to data theft and other security concerns. Consider enabling automatic updates so you never miss an important fix.

Staying Safe on Social Media

Social media is a powerful tool for staying connected with people and keeping up with the latest news or trends. It's also a dangerous tool when not used correctly. Criminals leverage these platforms to run scams, steal information, and manipulate opinions. You can keep yourself safe by avoiding common mistakes and following a few security practices.

Oversharing

People often share personal details without considering the potential risks. This is great for scammers, who use social media profiles to "mine" for information. This simple technique helps them discover someone's interests, location, job title, and names of friends and family. They use these details to build trust and create personalized scams that seem legitimate.

Security Tip: Limit what you share and set your profiles to private. Never post anything confidential about yourself or anyone else.

Fake Profiles

Scammers often create fake profiles by stealing photos and names of people you know. They'll then send you a friend request, hoping you'll accept without thinking. Once connected, they gain access to your network of friends, family, and co-workers, and can see all your private posts.

Security Tip: Thoroughly vet all requests to connect and report suspicious profiles immediately. Only connect with people you know and trust.

False Information

Disinformation is false information created specifically to deceive people. It is often designed to evoke feelings of anger, fear, or outrage, so you will share it instantly without verifying the facts. Misinformation is inaccurate information that people share because they believe it is true. Both can cause serious harm.

Security Tip: Think critically when you encounter emotionally charged headlines and content. If you're unsure if something's true, don't share it.