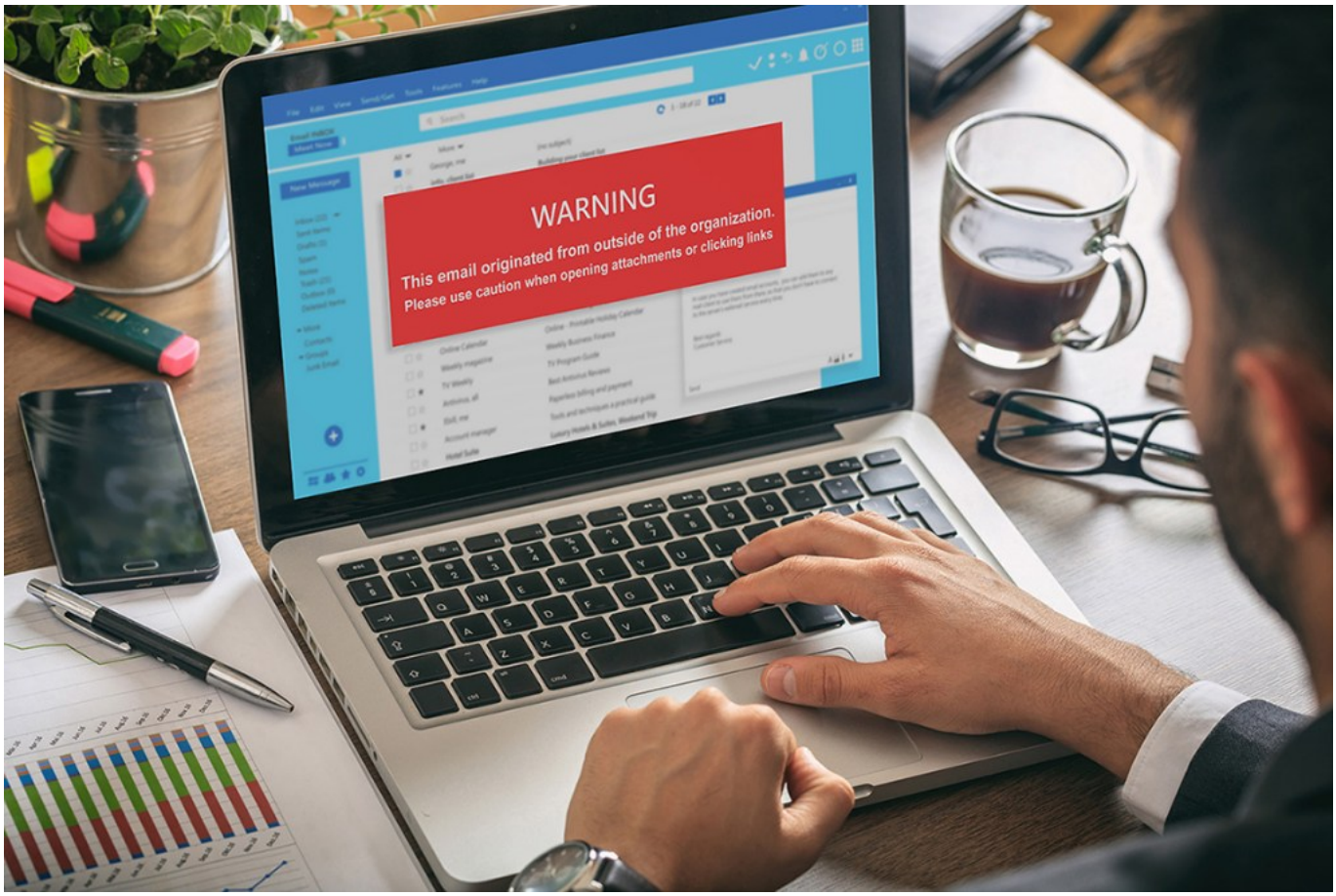
Cybersafety tips: How to spot a scam.



There are so many different kinds of online scams that it may seem impossible to guard against them all. However, if you keep in mind that the end goal of nearly all scams is to get you to reveal personal or financial information, you can learn how to spot a scam and keep your information secure.

Here’s how to spot some of the most common online scams.

Phishing Scams

A phishing scam is when fraudsters pose as an institution or business you trust, like your bank, school, or favorite store (for instance, many phishing scams involve Amazon). Usually, you’ll receive an email that says you need to update your personal or payment information and includes a link for that purpose. Unfortunately, this links not to the institution they claim to be, but to the cybercriminals stealing your information.

Some other typical phishing messages include:

- Your payment method was rejected, and you need to update it
- Here’s an invoice for your recent purchase (which you didn’t make)
- There’s been suspicious activity on your account

Other signs of a phishing email:

- Grammar and spelling errors
- The sender’s email address does not match the company
- Attachments (most legitimate companies do not send information via an attachment)

What to do if you receive a phishing email

First, never click on any links or attachments in the email. If you have an account with the company, go to your legitimate account site and check if there are messages or notifications related to the subject of the email. If not, it’s most likely a scam.

Remember, legitimate institutions and companies will never ask you to reveal sensitive personal information, like passwords, account numbers, or your social security number in an email.

Tech Support/Antivirus Software Scams

With tech support or antivirus software scams, fraudsters seek to convince you that something is wrong with your computer and that they have the answer to fix it.

In these scams, you receive a pop-up warning or email that tells you your computer has been infected with a virus or multiple viruses. The scammer encourages you to download software that will fix the problem or an app that will allow them to access your computer remotely and fix it, for a fee.

These scams are a double threat. Criminals get your credit card information to pay for their fake services and, in some cases, they also get you to download malware that will infect your computer.

To avoid these scams, make sure you have real antivirus software that will protect your computer. Also, be suspicious of difficult-to-close popups with dire warnings of viruses that must be immediately remedied (known as scareware).

Online Shopping Scams

Cybercriminals have become more and more sophisticated at impersonating legitimate retailers. **Fake shopping sites** look like the real ones, but may have a URL that’s just one letter or symbol off. You may see an ad on social media with an amazing, too-good-to-be-true deal, click through to the site, and then attempt to purchase the item. Because it’s a scam, however, all that happens is you give up your credit card information … and receive nothing in return, but trouble.

Another online shopping scam is called **formjacking**. This occurs when a cybercriminal hacks the payment system of a legitimate shopping site. After you choose an item to purchase and click to the payment page, you are taken to a fraudulent site that will steal your credit card information.

To avoid these scams, awareness is key. If you see deals that are too good to be true, they probably are. When shopping online, go directly to trusted sites rather than clicking through ads. Always examine the URL carefully to be sure it's legitimate. And even when you're shopping on favorite, trusted sites, examine the payment page URL before entering any credit card information; form-jackers usually slightly alter the legitimate site URL.

While these are some of the most prevalent online scams, there are dozens more. To protect yourself, remember:

- Never click on links in unsolicited emails or texts
- Never give your personal or credit card information to anyone claiming to be from a bank, company, or government agency without verifying their identity first
- Use strong passwords and change them regularly
- Install virus protection from a reputable source
- If it sounds too good to be true – a great deal, a message that you've won the lottery, a vacation or free gifts – it probably is
- You can report scams to the Federal Trade Commission at https://reportfraud.ftc.gov/ or by calling 1-877-FTC-HELP (1-877-382-4357)

If you stay alert and educated about online scams, you can keep your information safe from cybercriminals.

Concerned about cybersafety for your business? The Federal Communications Commission (FCC) offers these 10 Cyber Security Tips for Small Businesses. You can also talk to your local, independent agent for advice on keeping your company's information secure.