How to Protect Against Phishing Scams

Norton Antivirus

A phishing scam is a type of fraud that can come in many different forms. These scams not only employ various online techniques such as fake emails and pop-up ads but can also include phone calls. The people behind these scams often use fear tactics in order to get their victims to take the bait.
Phishing is essentially an online con game, and phishers are nothing more than tech-savvy con artists and identity thieves. They use spam, malicious websites, email messages, and instant messages to trick people into divulging sensitive information. Banking information, credit card accounts, usernames, and passwords are just some of the information phishers seek to exploit.

5 common phishing scams, and how to protect yourself from them

Since phishing scams are designed to appear as if they come from reliable sources, it is smart to know the difference between real and fraudulent messages and how to spot some of the clues that a message may be a scam. Here is a list of five common phishing scams and ways to help protect yourself against falling for them.

1. Email phishing scams
An email phishing scam is a fraudulent email message that appears to be from a person or company known to the victim. It attempts to illegally gather personal and/or financial information from the recipient.
A phishing message typically includes at least one link to a fake website, designed to mimic the site of a legitimate business. The message entices the recipient to provide information that could be used for identity theft or online financial theft.

How to help protect yourself against email phishing scams:

- Do not click any links or download any attachments in the suspicious email. Instead, open up your web browser and go to the website in question by typing it into the URL bar.
- Be vigilant and pay attention. Phishers have been known to use real company logos to make their communications seem legitimate. They also use spoofed email addresses, which are similar to the actual company's address. However, the address may be misspelled slightly or come from a spoofed domain.

2. Vishing scams

Vishing (voice or VoIP phishing) is the voice version of email phishing. "V" stands for voice, but otherwise, the scam attempt is the same. It is a phone scam in which individuals are tricked or scared into handing over valuable financial or personal information to scammers.

How to help protect yourself against vishing scams:

- Never give personal information over the phone. Hang up, look for the number of the company on their website, and call them directly to make sure it was a legitimate call and request.
- Never call the number the caller provides. When looking up the company website, make sure it is legitimate. Fake websites often contain misspellings and other telltale signs.

3. Tech support cold call scams

Tech support cold calls are when a scammer calls a potential victim claiming to be from a reputable security company. They lie and say they found malware on the victim's computer.
The criminal pretends to offer a solution by getting the user to install a type of remote desktop software. This allows the attacker access to the computer in order to install real malware. In addition to attempting to install malware on the machine, these scammers will often ask for a fee to "fix" the issue.
How to help protect yourself against tech support call scams:

- If a person calls claiming to work for a specific, well-known company, look up the phone number online and tell them you will call them back.
- Never allow remote access to your computer.

4. Pop-up warning scams

Pop-ups occur when someone is browsing the internet and sees a small graphic or ad appear on their screen. Usually, pop-ups are related to the content being viewed and link to another website with similar content or merchandise related to the content.

Malicious pop-ups can be terribly intrusive, making it difficult for the user to close the pop-up window. These pop-ups may display a message stating that the computer is infected with malware and offer a phone number for help with removing the malware. Often, the cybercriminals make pop-ups look like they come from a trusted source, such as our own Norton products, in hopes of appearing to be legitimate.

How to help protect yourself against pop-up scams:

Examine the message closely. **Look for obvious signs of fraud such as poor spelling, unprofessional imagery, and bad grammar.**

Remember, when in doubt, **never click on the pop-up. Instead, open up your antivirus software and run a system scan.**

Norton pop-ups **will only appear within the interface of the Norton Security Dashboard, and never from a web browser or other program.** In addition, **Norton customer support will never send users unsolicited pop-ups stating that they will fix a user's computer if given remote access.**

5. Fake search results scams

Fraudulent companies frequently use paid search ads for their "support services" as if they were legitimate, well-known companies. These paid listings can appear at the top of a search results page, a prime location. These results, which can look like the real thing, can promise support offers that seem too good to be true in hopes of luring in a victim, whose top concern is to fix their computer. Unfortunately, when you click on the ad, malware may begin to download to your device, compromising the security of your information and adding to your computer woes.

How to help protect yourself against fake search results scams

- Examine the URL closely. Creators of fake websites will sometimes try something called typo squatting, where they register a domain name that looks similar to the URL of the legitimate site they're duplicating.
- Use a secure search service, such as Norton Safe Search, to know if the site you're about to visit is safe.

What to do if you've been scammed

If you think you've been the victim of a phishing scam:

- **Change your passwords**. Your computer, financial institutions, your Norton Account, and any other password-protected websites that you visit should be updated.
- **Run a Full System Scan** for viruses on your computer.
- Contact your bank to report that you may have been the victim of fraud.
- Use Norton Power Eraser to scan your computer. It can help detect more complex threats than a traditional antivirus program may be able to.