Protection from online scammers and hackers

You might need a nerd if…

- You want to learn more about online scams, how they work, and how you can stay safe
- You gave your personal details to someone online, and you're now concerned you may have fallen prey to a phishing scam.
- You're looking for a friendly and trustworthy local computer technician to install malware protection software on your desktop or laptop
- You fell for an online scam or phishing scam (don't worry, it can happen to anyone!), and you want to make sure your computer is safe from follow-up attacks

The state of online scams and phishing scams in 2022

In the United States, one in ten adults will be impacted by an online scam of some kind this year. In 2022, phishing scam attempts (that's an online scam where a cybercriminal tries to steal your personal data) grew by over 60 percent compared to the year before. Companies aren't safe either. Four in five businesses experience attempted payment fraud each year, the Association of Financial Professionals reports.

Whether we like it or not, we live in risky computing times. Nerds On Call has been serving private and commercial customers for close to two decades now. In that time, we've seen the cybersecurity landscape transform. Online scams and

“viruses” (as they were collectively cataloged back in the day) were once more a mild nuisance than a serious threat. In 2022 malware, online scams, and phishing scams, in particular, can cripple a business and lay waste to your personal privacy, security and finances.

But here is where things get a bit rosier. There are ways — powerful and effective ones at that — to significantly reduce your chances of being caught by an online scam or malware attack. You also have powerful nerds-friends on standby to help you! If you’re worried that your computer, your privacy or your data are unsafe, give us a call at 1-800-919-6373, or fill out our contact form. We’re a trusted company and offer a fully mobile service; so we can come to you!

On this page, we’ll look at the kinds of online scams and phishing scams you may encounter. Then we’ll give you some simple and practical steps you can take to stay safe.

What online scams are out there?

Unfortunately, there are many and they change all the time. For an up-to-date list of trending online scams, it’s a good idea to bookmark the US Federal Trade Commission’s Scam Alerts page.

Here we’ll talk about the three broad categories of online scam you should know about.

Phishing scams

A phishing scam is an online deception carried out with the intention to steal private and sensitive information like credit card numbers, and passwords. Contemporary phishing scams often revolve around offering the potential victim a great time-limited deal. This “offer that’s too good to refuse” may, for example, be cheap health insurance, or lower interest rates on credit card debt.

In another phishing scam variant, the cybercriminal poses as a government employee, often invoking fear about impending tax problems or criminal repercussions to pressure their target into sharing their social security number.

Direct theft online scams

In these kinds of online scams, the malicious party isn't going after data; they're making a direct attempt scam you out of your money. As you can imagine, these vary significantly. Many involve the sale of fake products on e-commerce platforms. For example, you might make on online credit card payment for product that simply doesn't exist. Or you may receive an inferior product that doesn't match the advertised description.

Perhaps the most emotionally devastating kind of online scam is the so-called "romance scam." In these online scams, the cybercriminal posts a fake dating profile. After luring someone in, they try to create the illusion of a romantic relationship. Their ultimate plan is to build trust, gain direct emotional influence, and then pressure their target to send money to help them. People lost over $300 million to romance scams according to 2020 Federal Trade Commission data.

Software-mediated scams

Some online scams use software to steal your data. In these situations, a scammer will try to convince their victim to install software that conceals remote-access tools. Unbeknownst to you, the software will hunt for your sensitive data and send it to the cybercriminal.

What can you do to stay safe from online scams?

You aren't helpless against these scams! Far from it. There are preventive measures

you can take right now to stay safe from online scams. Nerds On Call can help too with a range of powerful cybersecurity services. Let's look at both now.

Here's what you can do

- **Trust carefully and confirm your sources:** Avoid clicking on links sent to you online, even if it *looks* like an official email. Don't give your data to anyone over the phone, even if they *sound* official. Instead, confirm by calling the bank or company directly. Be sure to get that number from an official website. Check the URL closely and remember that many phishing scams are built around fake websites. Never use a phone number, link or email address supplied in the questionable email or text.

- **Exercise common sense:** If a product or price tag looks too good to be true, it probably is. If you see a product online and it's *exactly* what you were looking for, take a moment to see if you can instead buy the product locally and face-to-face. That way, you have proof that it's real! Failing that, read reviews carefully and use sites that guarantee verified seller identities.

- **Don't rush:** Here's what 95% of phishing scammers will do when they approach you for your personal data. They'll rush you. Their goal will be to catch you off your guard so that you share your valuable data *before* that suspicious part of your brain kicks in and asks questions. If someone tries to rush you to a decision, react with extreme suspicion.

- **Recognize the red flags:** In TV-land, online scammers are clever and cunning — and sure, there are those – but the vast majority of online scammers use simple and predictable methods. If you see any of the following, assume it's probably a scam:

    - Any unexpected text or email informing you that you've won a prize.

    - Someone in your family contacting you online and asking for money using odd-sounding or uncharacteristic language.

- Any message that starts with a generic form of address like “Dear Sir or Madam,” or the infamous “Hi Dear!”

How Nerds On Call can help with online scams and phishing scams

Here are some of the ways Nerds On Call can help you stay safe from online scams and phishing scams. We can:

- **Scan your computers for malware:** Worried you might have been tricked by an online scam or phishing scam to install software you shouldn’t have? We can run a full diagnostic on your computer to make sure its free of malware infection. Remember, we’re a mobile repair and support service – we do housecalls.

- **Equip you with greater malware and online scam awareness:** If you feel you’d benefit from solid and trustworthy advice about online scam and phishing scam prevention, just give us a call at 1-800-919-6373. We’re here to help.

- **Help you set up useful services:** Credit Monitoring agencies like Experian, TransUnion, and Equifax can help you monitor your finances for unusual activity. We can help you install these great online scam protection services on your smartphone or home computer.

Worried about online scammers? We can help keep you safe.

If you’re worried about online scams pick up the phone and call us at 1-800-919-6373, or here’s our contact form.

Why Nerds On Call? We're a trusted company; we've been delivering quality technical support to home and business computer users since 2004. Best of all, we offer a fully mobile service! One of our trained technicians can come to you with a wide range of technical support and online scam prevention services.

Questions we're often asked about online scam and phishing scam prevention

What are the newest online scams?

To keep tabs on emerging threats, it's a good idea to check out the US Federal Trade Commission's Scam Alerts page.

How is a phishing scam different?

A phishing scam involves the theft of your data. A scammer will then use that information to steal your money or identity at a later date. If someone you don't know asks for your sensitive data, it's best to assume it's a phishing scam attempt. If this happens, immediately end the conversation, close the offending email or exit the website. Don't click on any links. Directly notify the bank or company the scammer claimed to represent.

Will anti-malware software keep me safe from online scams?

Anti-malware software is always a good idea, and good software will detect suspicious software on your machine. However, many online scams don't involve

software. Your best protection is to stay alert, use your common sense, and if in doubt ask someone you trust for advice.