# 17 Common Online Scams

*https://www.broadbandsearch.net/blog/common-online-scams*

We all remember the first time our parents sat us down and told us not to talk to strangers. It might not have made sense at the time - as kids we live in a fantasy world where everyone is our friend - but as we get older, it's easy to see all they were doing was trying to protect us. We share this world with many sinister souls.

In person, it's easy to see when someone is up to no good. However, as the world continues to digitize, the dangers that lurk are no longer contained in dark alleys and bad neighborhoods. Instead, they're in our email inboxes, our favorite websites, and our social media accounts.

Cybercrime doesn't threaten our lives and physical well-being, but it can do irrevocable harm to our financial stability and peace of mind. Of course, no one thinks they can become a victim of an online scam until it happens to them, and even the best of the best sometimes slip.

Staying safe online requires getting into the minds of cybercriminals, and that means identifying and understanding the scams they run.

Below, we've outlined the 17 most common online scams, and while this list is far from exhaustive, it should give you a good idea what to look out for so that you can use the Internet in a fun and safe way.

## Phishing

This is perhaps the most common form of online scam out there, largely because how well it works. Essentially, phishing is cybercriminals' attempt to get you to give them your information. Usually, phishing is done via email, and these emails are designed to look real.

For example, a phishing email could come from someone you know who has had their email account hacked, making it seem like the email is real.

Another thing that could happen is that the email could be made to mimic those sent by organizations you know and trust. In these instances, the emails look so real that it's easy to think they are legitimate, which is why we need to be so vigilant.  This is called "*spoofing*."

One of the best examples of this was the Google Docs phishing scam from a few years ago. In this instance, the email invited you to edit a doc, and it worked within Google's system, so it looked about as real as it could get. However, by agreeing to edit this document, users were granting a third-party software the right to read your emails and access your contacts. This gave the hackers access to sensitive personal information, such as bank account and credit/debit card numbers, as well as your social security number, which can be used to steal pretty much everything from you.

Phishing scams come in all shapes and sizes, though. For example, some may tell you that you're at risk of being charged huge fines by the IRS, or they may even say that someone else has hacked your account, but they will all tell you to give your information, usually right away, so that you can "stay safe." But all they are trying to do is create a sense of urgency so that you succumb to the scam without thinking.

Because of the diverse forms of phishing, it's hard to fully protect yourself. The best defence is to double check who is asking for your information. If it comes from  someone you know and it feels weird, reach out to them to find out if they really sent it, and when in doubt, just don't click.

# Spear-phishing

This is essentially the same thing as *phishing*, but the difference is that the hackers aren't after your *information*. Instead, they're usually looking for you to provide *access* to information for which you have privileged access. The classic example of this is the spear-phishing attack that managed to hack the *Democratic National Convention*.

If you are someone who has been trusted with information, make sure to follow your company/organization policies. It's unlikely someone you've never met will ask you for access without consulting you first, and you will surely be rewarded if you deny someone because you were concerned with fraud.

# Smshing

Another variation of phishing is *smshing*. It works in essentially the same way except that the fraudulent message will come through as a text message. It may come from one of your contacts or pretend to come from an institution with which you normally associate. Again, if it feels random - meaning you've done nothing to solicit this information - then leave it alone. Remember: when in doubt, don't click!

# Shopping scams

This particular type of scam is rather difficult to prevent merely because of its randomness. Essentially, these scams are based around companies that pretend to sell you products they have no intention of ever sending you. You may get a confirmation email after you pay, and they will certainly take your money, but the product will never arrive.

These scams will sometimes arrive to you via email or social media, but they will always direct you to a third-party eCommerce store. They will often offer high-end, luxury items at a very low price (a red flag) and they will usually demand payment via electronic funds transfer. You may also find these sites if you search for specific items.

If you're lucky, the worst thing that will happen is you'll lose the money you spend. But if you gave your credit card information, there's a good chance those who set up the scam are going to try and use it to make further purchases.

If you find yourself shopping on a site you've never visited before, it doesn't automatically mean it's a fraud but you should do some research. Look for customer reviews, see if these products are being sold elsewhere, and if you're really unsure, consider trying to contact the company. Not being able to reach someone is a big red flag that the site is really just a fraud. Also, check to make sure the site is secure (the URL starts with "https" and not just "http") and try to only spend money on sites that use secure payment platforms, such as PayPal and credit cards. This will help ensure your money is going to the right place.

# Nigerian Scams

This is one of the oldest online scams in the book, but shockingly, it still gets people. It's called the *Nigerian* scam because the first versions of it were sent from someone in Nigeria, but nowadays you can get emails from pretty much all over the world, and they all say the same thing. The term 419 comes from the designation this scam has received in the Nigerian legal code.

Essentially, in this scam, someone from a wealthy family in Nigeria, or some other West African nation, will reach out to you because they need help moving their fortune out of the country. They promise to wire you a bunch of money, but they will tell you that you need to first cover some of the fees involved in the transaction. You're promised a portion of their fortune for your help, but obviously this is never going to happen.

This type of thing is ALWAYS a scam. If you get this email, just delete it and tell your friends about it when you're at happy hour later that week.

## Bitcoin and Cryptocurrency

Cryptocurrencies, the most famous being Bitcoin, have taken the world by storm. They are cool, exciting, and often times quite valuable. However, few people truly understand how these things work, and cybercriminals are more than willing to use this ignorance to steal some money from you, or worse, all your personal information.

Most of these scams will encourage you to make an initial investment in a company that is about to go up for an Initial Coin Offering (ICO). In exchange for your money, you'll get a stake in the company, and this, the hackers will claim, is going to make you rich.

Sometimes these companies do actually exist, but the coins they are selling are either worthless or high risk. But most of the time, these companies are fictitious, and your payment will go towards nothing. Plus, if you do this, whoever contacted you will have your information, which they can use to rob you even more.

## Fine Print Scams

The fine print has the power to ruin us all. Nearly every online service we use has a set of terms on conditions to which we must agree, and they are usually longer than any

book we've ever read. As a result, most of us just click "Yes" or "I agree" without putting too much thought into what we're doing.

However, all too often, less reputable companies will put things in the fine print that give them the right to take more money from you. For example, you may sign up for some sort of subscription, and in the fine print it might say that after three months you will be charged an additional service fee, which is usually exorbitant.

As a result, when you're signing up for something, especially from a company you've never heard of before, make sure to do your homework. If you don't have the time to read everything in the terms and conditions, then at least Google the company to see if anyone else has had a problem. If they have, there's bound to be a complaint out there warning you to stay away from the company, and this little bit of research can save you a bunch of money and problems down the road.

## Fake Debt Help

Debt is a huge stressor in most people's lives. As a result, when someone comes in and offers to help you get rid of your debt quickly and easily, it's tempting to want to at least listen to what they have to say. However, as we know, taking shortcuts cutting corners gets us nowhere, and if you fall for this scam, you could be in serious trouble.

Essentially, these scammers will tell you that they can work with your creditors to help you lower your interest rates or even forgive some of what you owe. However, to gain access to this premium service, you need to pay an upfront fee, which obviously goes nowhere.

This scam works largely because it targets those who are most desperate and who are most willing to seek an alternate solution. However, if you find yourself in this situation, know that there's always a way to make things work that is safe and legal.

## Digital Kidnapping

This sounds scary, but it's not kidnapping in the traditional sense. Instead, in this scam, hackers will take control over one or all of your social media profiles. Then, they will

contact you and demand payment for access to be returned.

In some instances, they may threaten to post damaging content or harmful material, and this often has enough of an impact on people for them to open their wallets.

If this happens to you, the best thing you can do is contact the relevant social media platform and alert them that you've been a victim of fraud.

## Bad Downloads/Fake Antivirus Software

When you simply view content on the web, the files you're looking at technically don't get onto your computer. Instead, they are simply displayed from the relevant servers onto your browser. However, when you click "download," those files are in fact loaded onto your hard drive, and if you're downloading from sketchy sites, you can end up with some pretty nasty software on your computer.

One of the most common things you can get is malware, which is essentially software designed to collect information from your computer. It usually disrupts the function of your computer, and if you catch it in time you can get rid of it, but it might be too late.

Another piece of software you can download unknowingly is ransomware. This software will essentially lock you out of your computer and demand you pay a certain amount to get back in. DO NOT FALL FOR THIS. Instead, take your computer to a specialist, of if you know how, restore your computer to a point before the download.

Sometimes, hackers will work this scam by sending you a pop-up saying you're computer has been infected with a virus. In this same popup, you will be instructed to download software that will protect you but that will actually install something malicious on your computer. Again, when in doubt, don't click.

## Dating and Romance Scams

Loneliness can do remarkable things to the human psyche, and unfortunately, cybercriminals know this and are willing to prey on this weakness. These soulless

hackers will make an online dating profile and work to build a relationship with you. Then, after some time, they will start asking you to send them money, which you will be tempted to do since you've grown to care for this person.

It's easy to say you won't fall for this, but you never know. The best thing to do is to remember that you should never, under any circumstances, give money to someone you've never met in person.

## Fake Lotteries

Another common scam you will encounter online is what is known as the "fake lottery" scam, and it's exactly what it sounds like. Someone will contact you, usually via email, but it could also come via social media, text message, or even as a pop-up ad, telling you that you've won some sort of large lottery, usually in another country. However, to claim your "prize," you will need to give up some sensitive information, which should be a big red flag.

When you get a message such as this, just think back to when you may have entered some sort of lottery. If it's from a country you've never been to, then this is obviously a scam. But remember, if someone is offering you lots of money for doing nothing, there's a good chance they are up to no good.

## False Surveys

Surveys have been around for ages, and they are useful ways for companies and other organizations to gather information about their audiences. But if you are asked to give up information to take a survey, this is most likely a scam. Only take surveys that come directly from organizations and institutions you trust.

For example, if you bought a product from a company and receive an email from them asking for a survey, this is probably okay. But even so, you should never be asked to give away things such as your address, social security number, account information, etc., so if this is what's required to do a survey, turn and run as fast as you can.

## Mystery shopper (and other work from home scams)

This is one where the mantra "if it seems too good to be true than it probably is" applies more than ever. In this scam, someone will contact you saying that you can earn hundreds of dollars a day doing nothing more than shopping online. However, to get started, you will need to pay, upfront, for your "training" materials, but after you pay, you'll never hear from anyone again.

But this scam comes in other forms. Scammers know how much people like the idea of working from home and they prey on this desire, as well as the wish we all have to make lots of money doing pretty much nothing. However, the world doesn't work like this, so approach any offer promising lots of money for little work with tremendous caution.

## Account Failure/Problem

If you get an email from a service you use telling you there's a problem with your account that you need to fix right away, stop and search online for an explanation. If you can't find one, it's probably a scam, but you can also call the company to see if there is really an issue.

A good examples of this scam is that which occurred with Netflix. In this case instances, scammers claim there is a problem with your account, and they ask for your information to fix it. Specifically, Netflix users were told there was a problem with their payment information, and they were asked to re-enter it so that they could keep their account active, which handed credit card information right over to the bad guys.

There are countless scams like this one, so make sure to do due diligence before filling out forms with your personal information.

## Fake Charities

This particular scam makes it easy for us to be really cynical about the world. Essentially, scammers will ask you to donate to charities, especially after a large natural disaster or catastrophe, but these charities don't exist.

Instead, the money goes straight into someone else's pockets. When a major event does happen, only donate to reputable charities such as The Red Cross. Typically, during these times of elevated giving, the authorities will publish a list of approved charities (https://www.consumerreports.org/charitable-donations/best-ways-to-help-in-aftermath-of-a-natural-disaster/), so make sure to reference this resource before sending money to anyone claiming to help.

## Free-stuff Scam

Who doesn't love free stuff? Of course, most of the free stuff we get, such as pens, t-shirts, and coffee mugs, is essentially worthless, which is why it's free. However, if someone says you can get a free iPhone or brand new TV by doing nothing more than handing over some personal information, this is a scam. In some rare cases, you may actually get the item, but not until after you've given up something far more valuable.

Another common form of this scam is related to travel. For example, scammers will offer you a free stay in a hotel or a free flight, and this is a tough offer to resist. You must understand that there is no reason for someone to give these things away for free other than to steal from you.

## Pre-Approval Scam

When going through times of financial stress, it might be tempting to respond to an offer for a credit card for which you've been "pre-approved." Typically, these deals include high credit limits and low interest rates, which make them all that much more appealing. But the catch is that you will need to pay all of the fees upfront, which no credit card company will ever ask you to do, even if they do charge you annual fee. Many credit card companies do this, so it's easy to think these fake offers are real, but no one will ask you to pay these upfront.

## Digital Greeting Cards

Although not as popular as they once were, greeting cards are still a fun way for people to communicate with one another. However, if you're not careful, opening a greeting card from a scammer will trigger a download on your computer that can leave you with a

malicious piece of software that can steal your information and ruin your life.

These are tough to spot because they can sometimes come from people you know. However, if someone you haven't spoken to in years, or with whom you communicate using other mediums, suddenly sends you a greeting card, consider sending them a text or calling them before opening the email to keep yourself protected from whatever lurks inside.

# How to Stay Safe Online

Even if you are well-versed in all of these scams, new ones emerge every day, and it's impossible for us to stay on top of all the latest threats. As a result, it's important to learn how to stay safe. This doesn't mean you're guaranteed to avoid being scammed, but it will certainly boost your chances of avoiding the catastrophe of identity fraud. So, here are some tips to help you stay safe:


**Stick to the "if it's too good to be true, it probably is" mantra**. When someone offers you something for free, or if they're promising you a way to quickly and easily get rid of all your problems, pause for a moment. It's most likely a scam.

**Visit reputable sites and avoid clicking on ads and other weird looking links**.

**Verify contact information**. If the email address or phone number listed on a site doesn't work, there's a good chance you're dealing with something fake and will end up getting your information stolen.

**Check first.** If something strange comes from a family member or a work colleague, reach out to them and ask them if they know anything about it. Not only will this save you from falling victim to a scam, but it will help this person realize they are under attack so they can take the proper steps to get things under control.

**Guard your personal information with your life**. It's true we live in world where the lines of privacy are being blurred, but your digital identity is valuable and hard to recover. Only give out your personal information when you absolutely must, and only do it with companies and organizations you know and trust. You wouldn't walk down the street giving strangers your driver's license or bank account number, would you? Of course not, so apply the same logic when you're online.

**Use anti-virus software**. Although they're not perfect, antivirus software puts up a wall of defense between you and online criminals. It will notify you when you're accessing a suspicious site, and it can block downloads which can harm your computer. However, these programs are not a substitute for good practice, and even with these programs you can still fall victim to a scam.

**Use a VPNs and avoid public WiFi**. We all love logging into our local coffee shop's WiFi to work, check our email, and talk with friends. But these public networks open the door for cybercriminals to access our private information. A Virtual Private Network (VPN) can protect you, but the safest thing you can do is to avoid public networks altogether.

**When in doubt, don't click.** If you get an email or text message, or a pop-up, that seems even slightly suspicious, simply don't click. The potential reward is not worth the tremendous risk. Spend the time verifying it's real so that you can avoid catastrophe. If this means responding to a friend or colleague a bit later, it's well worth the wait.

## What to Do if You've Fallen for a Scam

No matter how educated we are and how carefully we tread the often murky waters of the internet, it's still possible to fall victim to a scam. If this happens, your course of action depends slightly on the type of scam. Here are some tips on what to do if the cybercriminals get to you:

## If you download malicious software...

Get rid of it. These programs are designed to be difficult to remove, so you may need to take your device to a professional. But if you're familiar with computers, you can start it in safe mode, and remove the bad software using an anti-malware program. Or, you can reset your computer to factory settings, or to a save point from before you got the software.

After you've done this, spend some time monitoring your accounts to see if any personal information was stolen. You could be proactive and cancel your credit and debit cards, and you may even want to contact a credit reporting agency so that you can prevent misuse of your information and alert them of potential fraud.

## If you send money to a person or fraudulent organization...

You might be out of luck when it comes time to get your money back, as most banks will invoke the "buyer beware" defense. However, you should still contact the authorities so that you can file a report, and in the event they catch the perpetrators, you could get something back. But even if you can't, alerting the authorities will at least help call attention to the scam and perhaps prevent others from falling victim to it.

## If you have your credit or debit card information stolen...

You should immediately call your bank and cancel the card. In the event someone took money from you, you can claim the charges as fraud and, depending on your bank's policy, you may get some of the money back.

## If you have your full identity stolen

Get ready to work. Identity theft is scary, and it takes a long time to fix things. Hopefully, you realize it before the crooks have been able to do anything, meaning all your actions will be preventative. However, if they have managed to take control of your identity, it could be a long time before things are right again.

# Conclusion

As you can see, scams are all over the Internet. They come in many shapes and sizes, and the damage they can cause ranges from the loss of a few bucks to complete identity theft. However, if you spend some time learning about the scams that are out there, you can develop a vigilant eye that should keep you safe from all that can harm you, allowing you to enjoy the internet for the immense source of information and entertainment that it is.