wizer-training.com

Top Six Scams You Need to Know About

Scammers are getting smarter so we need to stay up to date and protect ourselves from potential threats!

Fake Tech Support

Most of us are familiar with those annoying alarming pop ups that come up telling us something is wrong with our computer or that we have a virus and to call “this” number for help. Because we all know this old trick, cyber criminals have come up with even more ways to try and fool us.

1. The Real Fake Website - Have you ever accidentally mistyped the name of a website and ended up on a real website anyway? This is probably the easiest ones cyber criminals rely on since it is so easy for all of us to make this mistake. Here’s how it works:

You’re trying to contact the Geek Squad from Best Buy and visit their site by typing, "**www.betsbuy.com.**"

You see the Best Buy logo, find the support number, and call…*and now they got you.*

See, You went to **betsbuy** instead of **bestbuy** and landed on a site owned and made to look like the real site by cyber criminals. They have a support number for Geek Squad but it's not really going to Geek Squad. It's going to a cyber criminal ready to offer you fake support. All you need to do is give him access to your computer and a credit card!

2. The Real Fake Phone Number - Search engines are our friends. Billions of us use them every day to quickly find just about everything. Criminals are relying on this too and they are waiting for us!

You search for tech support and a ton of options are at your fingertips. You don't have time to go through all of them so you click on the one of the first few you see. Cyber criminals know this and market these listings to show up first in search engines. Then, they just sit by the phone and wait for the call…..from you. All they need is remote access to your computer and your credit card information to fix it for a fee. Not only do they have access to your money, they have access to anything on your computer and free range to add whatever files they want as well….like viruses….or spyware. Scary stuff!

3. The Real Fake Business on Google Maps - It is way too easy for scammers to add a legitimate looking business listing on Google maps. They'll use the real location and website but will use a phone number that is fake. I'm pretty sure you know what happens after this!

Though Google typically verifies if a business is legitimate by mailing a postcard, calling, or emailing a numerical code to enter into a Google website, the system is easy enough for scammers to bypass with fake addresses and phone numbers.

4. Real Fake Emails & Text Messages - Yes, the cyber criminals are here too. Why? Because that's where WE are! Similar to spam texts and emails, they'll send you a link or phone number to call to get tech support help.

5. Real Fake Phone Calls - They call YOU! - Now that pretty much most of the population has cell phones vs. landlines, the criminals have begun targeting you via a phone call. Just because your number may not be published, doesn't mean you won't get a call. These criminals have auto dialers that dial numbers at random and people are on standby waiting for anyone to answer. When you do, they claim they are from "The Apple Care

Team" and they received an alert that your cell phone or computer is infected. They offer to help and if you take them up on it, they got you.

6. Real Fake Browser Extensions - Extensions are made to make our browsing easier. There's some that track spending and offer discounts, grammar helpers, and now....real fake browser extensions. They can offer tech support at the click of a button or download malicious software when you install them. Either way, verify the publisher of any extensions you download and make sure they come from the Google Web Extension or Safari stores.

Oh, how the scammers love to scam, let us count the ways (and keep counting)...The important part is making sure you have the cyber security awareness necessary so that you can use your knowledge to your advantage to prevent these scams. (and save your hard earned cash)

Tips to Stay Safe

- We all get knocked in the arm by a kid or a cat while typing at some point but always check your spelling.
- Be mindful of the site(s) you are visiting and if something doesn't look right, don't click around. Verify its legitimacy first. Look for differences in the logo, grammatical or spelling errors, unbelievably free or very low priced items, phone numbers that don't match the actual phone number to the company. If you still aren't sure, contact the company.
- Always go directly to the official website to obtain the phone number. Don't call a number you saw on an ad or got by email, etc.
- If something is wrong with your computer and you know a trusted friend or family member that knows how to fix them, it may be worthwhile to ask them for help.
- If you need to, call the store you purchased the computer from or call Microsoft or Apple for issues with their operating systems. Just make sure you are calling the correct numbers!
- Do your part for your fellow humans and report fraudulent activity. Let's team up and stamp these criminals out!
- Block the scam phone number that called you and report the number to the FTC.
- Do not install any apps if you are not sure who the publisher is.

- Read a few reviews that have been verified from businesses when searching on social media sites or map services like Google Maps.
- Did you get a link sent to you for a support site? Instead of typing it into the address bar, type the link without the **www** into your browser's search field to see what comes up. You can even type the word "scam" after it to see if anyone else has complained about it!
- A legit help desk support team will not call you with an issue and they will not ask for your credit card information.

Gift Card Scams

Ahhh gift cards, the easy, no hassle way to give a gift that the recipient can purchase what they desire, yet another way that cyber criminals are taking advantage of unsuspecting people. Did you know that the most popular wish list item is a gift card?

Here's how the gift card scam works. Let's say you are a new employee, you get an email from your boss asking you to purchase gift cards to celebrate a win on a big project. You're new, you don't want to question the big guy!

What you don't know, is that the request is actually a phishing email from a cyber criminal pretending to be your boss.

This scam can also seem like it's coming from a good friend or even family members. So, if it sounds like a strange request, it probably is.

- Call to verify the request and sender.
- Don’t open gift cards from people you don’t know, they could be a virus!
- Don't scratch the codes and email, text, or give them away over the phone.
- No company, government entity, bank, or business will ever ask you to pay with a gift card.

Elderly Scams No More!

Nobody messes with my family, no way, no how! My guess is that you feel the same way about your parents and grandparents. All of us at Wizer do!

Let's face it, the older generation isn't as great as we are when it comes to technology which also means they lack information security training. Give them a break, they went almost their entire lives without it! Can you imagine?

Well, cyber criminals know this too. It's not rocket science to figure out. You guessed it, grandma is a vulnerable target. Picture this…

Grandma just learned how to use Gmail! (Way to go grandma!) She gets an email regarding her social security check that she is waiting for. She opens the message and a nice gentleman named Bob from The Social Security Office of Google promises her he can get her funds to her by tomorrow! Grandma is filled with joy that someone is being so nice! She really needs to get to the craft store so she can finish making her new grandbaby a blanket.

There's only one catch so that grandma can get her social security check faster, she needs to give Bob her banking information so that he can "do what he needs to do."

Grandma just lost her life savings. No baby blanket, no holiday gifts, no bingo night with the ladies. By contacting the Social Security Administration Office and verifying Bob's email address and phone number, Grandma may have been able to avoid losing all of her money. Here are some common scams and things everyone can do to avoid them:

- If you get an unexpected phone call from a family member asking to wire money or give personal information, hang up and call the number in your phonebook.
- Always consult with your doctor and only purchase from official websites that you are familiar with.

- If any antivirus popup shows up urging you to call Microsoft, it’s a scam! Don’t click on any link or call any number, just close the browser.
- Gift cards cannot be used to pay court fines, taxes, or medicine.
- Government entities ”never“ call people and demand payment.
- Don’t do business with anyone that just shows up at your door, and neverpay in advance. Always wait until all of the work is complete.
- You're a winner! The catch is, in order to receive your prize you will need to send money for taxes, shipping, or processing fees. Verify the company and phone number this came from.

Social Media Scams

We live in a world with constant evolving technology and social media platforms are being used to communicate with other humans more than ever. We’ve all been warned, we’ve seen a lot of scams, we’re ignoring certain types of messages, yet new scams arrive each day and it is important to stay "in the know."

Here are some of the top scams on popular social networks and how to avoid them:

The Fake Friend

Pretty easy to spot a direct message from someone without a profile picture claiming to be someone you already know, right? Wrong. People still accept these friend requests without verifying if the person actually sent the message. What’s worse is that it’s not hard to find an old post or profile information to send a personalized message like, “Hey Judy, I haven’t seen you in forever! Loved the vacation photos! Let’s chat soon!” Unfortunately, lots of people still accept the request and now have a new fake friend.

- See if the friend is already in your list
- Text or message them to see if they sent you a request. If not, tell them their account may have been hacked and to change their password.

See Who's Viewed Your Profile

I mean who wouldn't want to know who has been stalking their page? Mark Zuckerberg of Facebook has remained adamant that the See Who's Viewed Your Profile feature will never be available. You would think that's all anyone would need to know to know that anything else would be a scam but here we are…

You're scrolling through your newsfeed for the 5th time today, you see an ad that says, See Who's Viewed Your Profile, you click on it to install the app, allow the app access to your profile information, and then not only do they have your information, they'll gladly use your account to post even more ads, and worse, create a fake account and try to friend everyone you know in order to spread their agenda.

Now, you don't have to just go on Facebook for this....I found a website full of false info and clickbait just waiting for me by doing a simple Google search for this scam.

- If Facebook implements this feature, it will be automatically added in your settings and the majority of your newsfeed will be talking about it like it's going out of style. Do not trust anything else.
- If you see a false ad, report it to Facebook.
  You can always go straight to the source to ask questions about features in Facebook's Help Section!

The Long Awaited Facebook "Dislike" Button…is NOT Here

Nope, Facebook still hasn't implemented this feature and anyone or anything telling you otherwise, is lying. The closest you will get is the angry face emoticon.

It's a quick ad in your newsfeed, "click here to upgrade and add the dislike button", nope, don't do it. This scam works just like the "See Who's Viewed Your Profile" scam!

Great Deal on a Sweater

Instagram is a huge success due to rapid photo posting and many cyber criminals are copying product photos from popular retailers and pretending to sell items at great deals through Instagram. An unsuspecting buyer then clicks on the item, purchases it, and never receives it. After that, it's pretty

hard to track down the original post since you've probably gotten 100 more in your feed since you clicked. Can anyone say, #InstaSCAM?

Take a look at the link you are going to before you go! You wouldn't take a trip without pulling up a map!

Account Brokering

Buy this account for $45, comes with tons of followers, oh and it's not real but I'm $45 richer plus you just violated Twitter's Terms of Service against buying and selling accounts so good luck getting help. Not only are these scammers creating bogus accounts, they're running off with your money!

Simple way to avoid this...Don't do it.

Buy "Likes" and "Followers"This is actually a thing. Anyone running a business and marketing through social media knows that the way to get "seen" online is to have "likes" and "followers." This takes time but many people want to jump in and start making money right away so they try to purchase them to grow their brand fast. Here's the problem, buying this information can not only get you in trouble with most sites' TOS agreements, we can guarantee you won't get qualified "likes" or "followers." Most of them are bots anyway so upping your customer engagement game won't even work.

Just Don't.

Fake Checks

Ever had that moment when splitting up a bill with friends and you end up paying $75 for a $15 salad? Well, a fake check scam is similar but you wind up without the salad. Here's how it works:

1. A scammer pretends to be someone that will eventually need to pay you for something. Like for instance, maybe you are working with someone willing to buy your car on Craigslist.

2. You'll deposit their check into your bank account and you will see the money reflect in your balance.

3. The scammer will then claim they sent too much money by mistake and ask you to give back the difference.

The scammer might ask you to return the funds in a number of ways: in cash, by writing a personal check, by loading it onto a pre-paid or gift card, or through some electronic means, such as a wire transfer, automated clearing house (ACH) payment, or a person to person (P2P) transaction.

Of course, you will want to do the right thing and pay them! But, here's the loophole:

Even though you see the money in your account, it takes the bank anywhere from a week to a month to clear the check.

When the check bounces, you end up paying back the bank and any money you sent to the scammer. It's your loss, not the bank's.

Here's what you can do:

If you're selling something, accept only cash in person. If you must receive a check, verify who it is from by looking at the name on the check and asking to see photo identification. If it is from a business, call the company and verify its authenticity and make sure the company is legit by calling or verifying their website. If something doesn't feel right, don't deposit the check.

Online marketplaces are a great breeding ground for scammers.

Job Scams

We all know the painstaking process of finding a job. It’s time consuming and it takes a lot of rewriting your resume and cover letter to match a job description, filling out online applications, waiting for phone calls, trying to

schedule interviews….uhhhh need I say more? It's frustrating sometimes but it's something we all have to do at some point.

You know that feeling? The one where you get an email or a phone call regarding one of your many resumes you've submitted? "FINALLY," you think, "I've FINALLY gotten someone to reach back out, this could be the job I've been waiting for! I'm soooooo excited! You jump at the chance to sneak away so that you can answer that email because you want to be first in line for this job.

You desperately want something. You have been working hard to get it. You're going to jump at the chance to respond to a potential employer. You are vulnerable and cyber criminals rely on it!

Think about it, when you are job hunting you are sharing personal details with strangers. You may be opening attachments, filling out forms or even sharing your bank account info. What more can a cyber criminal ask for? They can post a job and use the personal information candidates share with them to steal their identity, or send candidates infected documents to their business or personal account.

Hackers especially like to target work from home candidates. Here's how it works. You are supposedly hired by a fake company, the hacker will send the you a check as advanced reimbursement for purchasing a company laptop. You will deposit the check to a personal account and will use a personal credit card to purchase a laptop from a link the hacker sent. Obviously this is a fake store and a week later the check will bounce, but you will not be able to cancel the credit card charge.