

How to Tell When (If) You're Being Scammed

It's unfortunate, but "scammer" seems to be the new profession for millions of shady characters across the globe. It's easy to do, highly lucrative, and nearly impossible to trace (and prosecute) particularly if the scam originates outside of the US. We simply cannot find or prosecute most scammers even if we do know who they are. And most (but not all) occur online (electronically) from foreign origins so there is no recourse whatsoever.

To help you understand when you might be getting scammed, I've devised a series of questions and "tells" for you to make note of whenever you feel like you might be getting scammed. I will warn you – it will be long, it will be detailed, it is not top 10 garbage you'll see on the evening news. I attempt to explain both the logic behind the scam and some of the behaviors you might encounter. There's no magic bullet or key to press to protect yourself. You have to use your head and not listen to the "pitch" – which a lot of people seem averse to these days. Don't be that person. Even the most intelligent, careful, thorough, and protected people can be hacked and fooled. It isn't **if** you'll be hacked, it is **when** you will be hacked remember that...we are not immune. All we can do is protect and mitigate the damage they cause. We can't stop it, but we can make it damn hard for them to succeed if we just try.

So, for starters, when you get a really, really obvious scam you laugh and say to yourself "who is dumb enough to fall for that" – the problem is, that's exactly the target audience. If they hit enough people, they will find someone kind hearted or gullible to exploit. In general, they don't want people who ask questions or are suspicious of scams, it is too much energy to waste for too little payoff. They want the low hanging fruit that will be easy to manipulate. Question. Everything.

Reminds me years ago of some old timers in my parent's generation. "I'm not doing anything online so I will never have any problem. I don't do email. I don't use Facebook. I don't do online banking." It of course sounds like wise logic at face value – no electronics, no hackers. Right? However, it's completely nonsensical as every bank, insurance company, and heck even the government DOES do things online and electronically *with your sensitive information*. So, while you may have isolated yourself in a technology bubble, no human who interacts with the world is protected because the world is electronic. The credit bureaus see every transaction you make, banks release information to the IRS regarding your finances, employes entire payroll systems are often online. You alone (are not alone) – you are exposed on many levels. This is referred to as your threat 'attack surface' – the more you put yourself out there, the more avenues you open for potential attacks. So, while there is some truth in keeping yourself offline will help you be safe, but in many ways, being isolated from what is happening in the real world (aka by not receiving alerts when your credit scores change, new bank accounts are opened, or debits appear on your accounts) you may be doing more harm than good. And the phone. Remember the phone. Phone calls are probably more dangerous than online banking because you have a human on the other end of the phone with a well-tuned script to lure you out of your money.

So, when thinking about scams, think of the concept of "attack surface" – where can they get me? Everyone out there has a whole bunch of your personal information, and a lot of it is public. Don't believe me? Google yourself. Add in the town and state. See what you can see. And that's just the **really** public stuff. Imagine what people with skills can find out.... we are all victims here. Most scammers want a few hundred bucks and then they move onto the next person. They don't want to be chased down for committing a felony, they want to be forgotten quickly because the person scammed is

embarrassed by it all and not enough money was lost to make it worth reporting. So, most hacks aren't very monumental, they scrape a little, take and run. So, it doesn't matter if you have \$2000 in your bank account or \$2million – we are all susceptible and perfect victims in many ways. In fact, most insurance policies, both business and personal, now have some provision for protection from cybercrimes. Yes, it's that common, and no, nothing is really being done despite what the extremely aged population in our government say they are working hard to protect us. They are light years behind the curve on this one (think about how they are talking about regulating AI – they are a day late and a dollar short on this one).

So, off we go!

Rule #1: Trust No One.

This is going to be difficult for a lot of good, honest, trusting people. Which I genuinely believe is all of us. But mark my words here – when it comes to money and personal information exchanges - always be cautious, and trust no one beyond arm's length. Be sure you are engaging in actual business, and that you initiate the exchange of anything (dollars, information, etc.) yourself. Do not let anyone pressure you into giving them anything, ever. No matter how convincing the story is. Just say no and ask yourself what the consequences might be if you did not complete the requested action. For example, if you are buying a vehicle and sitting in the showroom and the finance manager asks you for a credit card – ask yourself what the consequence of not giving him that card may be. In this case – you don't get a car. You don't go to jail, you don't lose access to something you own, you simply do not get what you are paying for. And believe me, giving that card to a shady car salesman is akin to a scam because they will make your life hell if you try to back out of a deal.

So--- When you receive a request online to provide your social security number or 'your password needs to be reset' or you lose access to (fill in the blank) – ask yourself what would you lose. Assess the request, look at the facts, and decide if the transaction is really worth it. Losing access to your Cable TV provider would be a small inconvenience. So refer to rule #1 and trust no one.

Rule #2: Trust Your Gut.

There's a relatively universal rule when it comes to scams of all shapes and sizes. ***If it sounds too good to be true, it probably is.*** And to clarify that rule, if anyone is offering you something in an exchange where you receive a significant benefit at their loss, it's probably a scam. New iPhone for \$45? Stolen. Get Free year of Cable TV just for filling out a simple form? Phishing. For just a one-time credit card payment of \$12 you will receive a million dollars in protection? Scam. Allow me to reiterate: ***If it sounds too good to be true it probably is.*** This should heighten your awareness, raise the hairs on your neck and put you on the defensive immediately. Trust your gut, be cautious and look for things that 'just don't seem right.' If you have ***ANY*** doubts or hesitations, cease the call, delete the email, throw away the mailer and ***call the company requesting this information directly from a phone book or public listing.*** Never, ever, ever, ever use the phone number a potential scammer may give you as they have engineered a fake team to look/feel/respond to your inquiry. They can fake flyers, mail, websites – anything and everything.

Rule #3: Is the Tone Threatening?

Another perfect scam is the “*perform this action or your account will be terminated.*” This comes in many forms, but they are all generally the same. “Change your password now by clicking here or you will never be able to access your money again. “OR “Your social security number has been compromised please call us at this number now” OR “This is the IRS, we have reason to believe you have cheated on your taxes, call us now to avoid penalties and jail time.”

Scammers are really, really good at playing on emotions, and particularly target the elderly who are not up to speed on the fast pace of technology and the ways of the world as they may exist today. Remember, much of our population conducted business face to face their whole life, only recently turning to “online” portals. It’s confusing, it’s ever-changing, and even the most tech savvy folks are taken back by the speed in which things change. Don’t believe me? You can pay for gas with cash, credit cards, your phone, and numerous other ways. For example you can tap a credit card on the pump, and you can even tap your phone on the pump and the magic of technology appears. Older people and those less technically inclined struggle with the actual pace of change, let alone when they are being targeted with a scam. Heck I work in technology and I don’t even understand how to pay for gas anymore (I use the Cumby’s App – I know it works and I get 10 cents off per gallon!).

Often times if there is a threatening action expressed in the message (you must act now, you must complete this action OR ELSE) it’s generally a scam. Yes, you can and will receive a legitimate message (we have not received payment for your cable TV bill and your account may be terminated) but there is always a main number of the company you are dealing with you can call and find out if it is an authentic request or a scam. See above...NEVER use the phone number on the email/mail in question. ALWAYS call the company main line from a directory (yellow pages, google, etc.). Then, when talking to a neutral party, you can inquire if the threatened action is authentic or a fake. So ask yourself “Does this even make sense?” first (if you pay all your bills you are likely never going to face a termination letter). If you are afraid of an outcome because someone planted that fear – it’s probably a fake. And heck, so what if your cable tv gets turned off, it’s not worth the money we spend in the first place...

Rule #4: Logos are meaningless.



Anyone can copy a logo, letterhead, phone number, email format – etc. Do not believe it just because it “looks” legitimate. One used to be able to look for grammatical errors and poorly formatted content and identify potential scammers – not anymore. The sophistication levels have increased to the point where you may not be able to tell a real communication from a fake one using just your eyes. Using this IRS logo does not mean I am working with the IRS. And AI can write a message in better English than I can. Again, if there is any request that seems questionable, disregard everything in the communication and call the company’s main phone line and ask if the communication is a) legitimate and b) how to rectify. If they cannot find an answer, into the trash the request will go. If the IRS really wants to find you, they will. But you need to do some due diligence and step outside of the request to find out if it is real. In cases where communications come from banks or other financial institutions, find a **real** statement or call the number on the **back** of your ID/Credit/Debit Card and inquire directly.

Rule #5: Never Click a Link in an Email

So here is where we have to take a commonsense approach – every email we get says ‘click here’ for more information. We are accustomed to it and its actually how legitimate businesses work these days. HOWEVER. If you are being asked for any uninitiated information (a password reset, address request, login credentials) – absolutely anything that requests personal information. Beware. Yes if you click the “Shop Now” button on an email you will be brought to a vendor website where you may be asked to login. Just – BE CAREFUL. You can always delete the email and log into the vendor site from a secure browser by typing in the web address...avoiding a potential misleading link. BE THE INTIATOR NOT THE SUCKER!

Rule #6: Always check the FROM of an email.

Perhaps the easiest way to tell a scam/fake message from the real deal is to look at the FROM line of an email. However this is not always clear to people either. DO NOT look at the name of the sender. This can be modified for any email account. What you MUST do is hit the reply button and look to see the actual email address the communication originated from. This has gotten more and more difficult as many corporations use mailing services so the mail may come from dfdfdfdfdfdnvnfnjnvdf@bankofUSA.com – it may look like garbage (and if so - its probably just what we call legitimate SPAM – marketing emails that are of little value from companies you actually do business with.)

But nine times out of 10 when you click that reply button you wont see johnsmith@yourbank.com you’ll see BernieEarnie@philspicklecompany.com (a stolen or hacked email from a legitimate company) or a Gmail/Hotmail/yahoo account – which certainly indicates an individual and not the company being represented.

If the email comes from customercare@apple.com you are probably in a good position. But be warned, it is very, very easy to change the email to look legitimate when in fact it is not. customercare@applecare.com, customercare@applecorporation.com, customercare@appleplus.com – or even customercare@apple.online or .net ---- so many emails are meant to look like that of the legitimate senders. So this rule *ONLY* will alert you to the most obvious scams.

You can also send a blank email to the sender, if it comes back immediately as undeliverable – probably a scam. There’s no foolproof way to know, just clues. To avoid having to actually communicate in a two way fashion with customers, most companies send from a noreply@company.com – again this is a totally legitimate business practice these days. So this doesn’t always work. You can also --- if you are technically inclined --- look at the source code of an email (aka the headers) and see its origins, but this is advanced level stuff. Hackers are really good at “spoofing” (aka faking) legitimacy so you should be very careful. Return to the golden rule of deleting the communication/request, hanging up the phone or throwing away the mail and contact the company directly, on your own terms, and ask about the legitimacy of the communication.

RULE #7: Use a credit card to pay for things

This isn’t a great “always” rule, but most credit cards will protect you in some way. You can dispute charges for example, report theft and fraud, and sometimes get your money back. Sometimes. Using cash, checks, Zelle or debit cards – since you do not pay fees (essentially with many fees you are paying

a premium for transaction insurance) you are NOT protected and have no recourse. So if you must pay for something, use a credit card. They don't want to get ripped off any more than you do at banks, but they also have a lot more room to make a profit at 29% interest. So they take a few hits on scams here and there to keep things moving along. Never, ever wire money to an unsubstantiated source. Never send cash or checks, and if they ask for (untraceable) gift cards, laugh at them while hanging up. The IRS is never, ever, ever going to ask you to buy a gift card from Family-Mart. NEVER.

Rule #8: Never buy anything of untraceable value

Because of the transient nature of gift cards (few are tracked, most are never redeemed, and they can be exchanged freely) they are a perfect choice of Theft-O-Currency – all a hacker needs is a number via email or off the back of that card and its just like cash. Amazon, best buy, whatever works, they can sell it for pennies on the dollar and make money. Even if they can get \$20 for a \$100 gift card (funded by you) they will make out. Buy low (in this case at zero dollars) and sell high. Take profits, run! Do not ever buy gift cards! And the same goes for Cryptocurrencies. I'm too old to understand them myself so the resounding answer is NO.

Here's a great scam: You receive an email from Cindy in accounting at your company. It says *"the boss wants you to drop everything you are doing, buy \$350 in Amazon gift cards for his kid's graduation part - just email them to this email address. Use your personal credit card and we will pay you right back, we are having a problem with our payment service today. -Cindy"*

You say to yourself "well, if the boss wants it, the boss gets it." So, you buy and send the gift cards.

Later you ask Cindy about the reimbursement for gift cards you haven't received, and she looks at you like you're crazy? You say "But your email said to!" and she says "I never sent that email?" – in these occasions one of two things may have happened. A) her email could have been hacked and a hacker simply emailed you from her account, deleted the email from her SENT account, and she was none the wiser. OR. The hacker could have spoofed her email to look like Cindy (but it really wasn't). They may have changed a letter or two in the email (Cindy@yourcompany.com could have been spoofed to cindy@yourcompany.net for example) and you likely wouldn't notice. What you should notice is – trust no one, anytime you are asked to conduct a transaction think twice, and never buy anything of untraceable value! If you did receive this email, pick up the phone and verify with Cindy that the request is legit. Because this type of stuff does happen in life – you may be bailing out your boss! So again, if and when this happens, pick up the phone and call Cindy to verify. DO NOT EMAIL her because SHE MAY NOT BE THE ONE LOOKING AT THE EMAIL! Now, I know what you're saying, we do this day in and day out so I can't call every time the boss wants something. No, you probably can't, but you are looking for suspicious or out of the ordinary activities (use your own credit card, the boss said to, we will pay you back). While it does happen in smaller offices that you may use your own credit card to buy something – make sure you at least use the corporate account! Validation with a real human you know goes a long way.

Now, in corporate America, this logic causes a ton of headaches, because to be fair they don't much care about you. They ask for anything personal they want to from mothers maiden names (nay, demand such things) and index your account by your social security number. Then they get hacked and say "sorry, here's a year of credit monitoring services we can get for cheap." They just don't care. And fighting with the corporate machine is an endless battle. But sometimes – you have to do it. When the cashier at the

grocery store asks for your phone number, simply say “no thanks”. Of course, you can’t escape a bank or a utility company asking for this info. Just be sure there is a reason, double check and validate the source, and think about it before sending.

Rule #9: Just because it is an invoice doesn’t mean it’s a *real* invoice.


This one is a real hoot. Someone just opens up a QuickBooks or PayPal account and blindly sends invoices to anyone and everyone they can find a mailing address for. Most businesses use an accountant or bookkeeper who simply pays invoices in a big pile and records the payments. They rarely know who the businesses are requesting payments – they just pay the total and record the transaction. This can come via mail, email, PayPal or even a blank envelope dropped off in person. The moral of the story here is know your vendors, manage your transactions, and actively communicate with accounts payable (or do your own books). What looks like a perfectly legitimate invoice may be from a company you’ve never seen/heard of or worked with before. A common scam is for people who own web domains to get a notice that the domain is expiring, when in fact, they do expire. The date is probably accurate and the web domain is one you really own. SO, you send a payment to renew. And this is only a half scam, some companies charge you \$200 for a \$20 service. A lot of folks are too hurried to pay attention (or don’t understand the technology) and just pay the bill. Geek Squad and McAfee are other scams commonly used. Sometimes these companies are so thrilled you gave them 10 times more than the going rate – they’ll actually register the domain for you legitimately and then hit you up with an overinflated bill next year. They just stole you as a customer and made huge unnecessary profits because you didn’t pay attention to what services you pay for. Happens all the time. And this scam isn’t even illegal. You can pay anything you want for a service – it’s all on YOU to decide who to do business with and what to pay.

Almost like magic – as I penned this very piece – I received a scam invoice from PayPal. It’s a real invoice, I can really pay it, they used my real email – but I have never done business with this company in my life. What do we never ever do – call the number on the invoice, then you’ll be dragged deeper into the scam and have to fight your way back to the top. Simplest action – don’t pay it, delete it. If it is real – someone somewhere is going to let you know. But scammers usually go away as quickly as they appear *unless they start to get somewhere*. If they can get you on the phone they have ways to trick you. One is a deep apology – OMG I cant believe I sent this invoice to the wrong client. We just charged your credit card. Give me the number and I will reverse that charge IMMEDIATELY! So you read off the number expecting a \$499 credit but in reality – you just gave away your credit to a stranger because of a fake invoice. You’re getting no credit. You just bought a Rolex for someone’s mistress...if you want to get crazy, google the phone number. Let’s not miss the irony that the invoice is from Bernie Sanders...I mean – seriously. They not only rip you off but also embarrass you...Bernie sanders is not sending you an invoice for “Ultimate Pro” ...he’s busy with his mittens.

Invoice from Bernard LLC

Bernard LLC Bernard Sanders 103 Aleo 8th Ave Rockingham, NC 28379	Invoice #5203 Issued : Apr 12, 2022 Due : Apr 12, 2022						
\$499.50 DUE							
✉ georggeorg177@yahoo.com							
Bill to rscimagery@comcast.net							
Items							
<table><tr><td>ULTIMATE PRO</td><td style="text-align: right;">\$499.50</td></tr><tr><td>1 x\$499.50</td><td></td></tr></table>		ULTIMATE PRO	\$499.50	1 x\$499.50			
ULTIMATE PRO	\$499.50						
1 x\$499.50							
<table><tr><td>Subtotal</td><td>\$499.50</td></tr><tr><td>Shipping</td><td>\$0.00</td></tr><tr><td>Total</td><td>\$499.50</td></tr></table>		Subtotal	\$499.50	Shipping	\$0.00	Total	\$499.50
Subtotal	\$499.50						
Shipping	\$0.00						
Total	\$499.50						
Note to customer Thank you for using pay pal. \$499.50 has been successfully send to patric smith. Same amount has been debited from your bank account . We are there to help you 24x7. If you want to cancel this payment calls us immediately at +1(888) 915-9175							

Balance due:



When in doubt? Google the company name and phone number. Its easy and free. I did just for kicks...Note how Bernard Corp doesn't come up. Other reports of the number being a scam do. Guess what this tells us? It's a dang scam! But you knew that by now because you're on to these thieves and their tactics. DO NOT ENGAGE. As you see below, you'll be directed somehow to another number or person (they may answer as Bernard LLC) and then blammo. The scam goes on. Don't fall for it!

About 80,500 results (0.40 seconds)

<https://800notes.com> › [Phone.aspx](#) › [1-888-915-9878](#) ⋮

[888-915-9878 / 8889159878 - 800Notes](#)

Jan 29, 2020 – 30 Jan 2020 | 1 reply ... Calls from a 916 number but gives an **888** number to call back. Caller: 916-330-3792; Call type: Scam suspicion.

20 posts · Left a partial VM about counsel calling to voluntarily take care of my "file". I'm thinkin...

[888-947-9175 / 8889479175](#) 3 posts Nov 15, 2018

[888-915-0208 / 8889150208](#) 17 posts Dec 30, 2021

[More results from 800notes.com](#)

Missing: [915-9175](#) | Must include: [915-9175](#)

Rule #10: Monitor Your Credit Card Activity.

Set spending limit alerts, heck, get notified of every transaction you make on your phone via text. Don't recognize a charge? Call in the militia and get your credit card company on the line *immediately* and report fraud. A lot of times you are protected if you didn't lose your card or hand out your credit card number willy nilly to a stranger with a good story. They'll usually reverse the charge if it is caught immediately (say, before the 77 inch TV they just ordered on your dime gets shipped out). Charges caught early can often be dealt with. Wait a month and you may find you're on your own. Part of owning credit is managing it like you would a big pile of cash. You'd never leave that cash unattended. Credit companies make it easy now to get text alerts, emails or even phone calls when something is charged to you card. This way you know in real time if you are purchasing items that YOU aren't actually purchasing.

Conclusion:

So, there's your top ten. Could these rules be wrong or up for debate? Absolutely. Is there any sure-fire way to keep from getting scammed? Absolutely not. But if we stop, think, and develop a critical eye toward people trying to take our money, we may be better at preventing the theft from happening. The bottom line here is when someone asks you for money or items of value: stop, think, assess, decide, and then act. Never act out of fear, threat, or punishment. Pay legitimate bills freely using known systems that work - and question everything else. What's the worst that can happen?

Rich Collins

Thirst Productions, LLC

<https://thirstproductions.com>