Common technology scams and what you can do about it

Scams take on many forms. But the goal is the same: to get your money or something else of value. Knowing this, the best way to protect yourself is to never ever give something of value or your personal information to someone you would not trust with the keys to your house. The exception is, of course, when you are paying them for a service that you requested and that was performed for you. For example: if *you call* a plumber to fix something in your house, you should pay; but if a plumber *calls you* to fix something, do not pay or let them on to your property. If *you call* your phone company to pay a bill with a number that you know to be legitimate, you are fine; but if the phone company *calls you* to collect a bill, do not pay.

Many, but not all, scams play on two desires: fear and greed. The scams that play on our fear try to make you think that some bad action will happen to you or someone you know, usually a close family member, unless you act quickly. Or they make you think something is seriously wrong with your property that can be fixed by calling a certain number or using the services of the person who told you about the problem. The ones that play on your greed make you think that you are entitled to some money, not always a large amount, and the person who told you that is there to help you get it.

With that in mind, a tell-tale sign of many, **but not all**, scams is this: *They* tell you have a problem you were unaware of, but *they* can fix your problem. Of course, 'they' refers to someone or something that tells you that you have a problem. Another tell-tale sign of a scam is somebody tells you something really bad will happen but if you just listen to them, and make a monetary sacrifice, this really bad thing won't happen. If you do nothing and it doesn't happen – and the really bad thing will never ever happen – the scammer will still claim that they saved you, so now you should listen to them because only they can save you from this new really bad thing or from any thing similar to the other really bad thing.

Below are scams that are done using modern technology. Knowledge of what they are can help protect you. But be aware, studies have shown that people who are aware of these scams are more likely to be a victim of a scam.[i] Knowing the scams can make you overconfident. (This same principle is what causes the most educated people to be the most susceptible to mental conditioning.) So do not ever think it cannot happen to you because you know better.

You can avoid many scams with these simple rules: (1) Never ever pay anyone by wire transfer, money order, pre-paid cards, or a virtual currency like bitcoin. Scammers want you to pay this way because there is no way to recover your funds. (2) Never ever pay a check or cash for any service that you did not request yourself because you knew you needed that service. (3) *Always* pay by credit card over the phone, no exception. Credit card companies can do a chargeback and get the money back. (4) Never agree to transfer funds between accounts over the phone, no exception. If you need to transfer funds between accounts, always do this in-person at your local bank or credit union. (5) Always remember that, while most people are good people, a significant number of people will find a way to abuse the system.

Many scammers are based in India because the government is not rich enough to do much about it and because there are enough English speakers there to make it possible. However, the money has to be routed through the United States somehow. The scammers often use bagmen to handle this.[ii]

Below are several scams. These are not all the scams that you could see. The focus is on scams related to technology. The description of the scam is purposefully generic so that it will cover the various forms the scam will take.

The fake security alert/fake tech support scam

This scam is now usually done by malicious advertising, or malvertising. The way it works is a scammer buys an ad through an advertising company. Scammers exploit the entire advertising system. Almost every single ad today has tracking code within it, to deliver more "relevant" advertising. The creepy, unethical tracking is a separate problem. But scammers exploit the greedy, unscrupulous advertisers. Instead of tracking code, scammers place code that redirects your web browser to a website under their control. They have other tricks to deliver the scam too. Sometimes the scammers will hack a website to do all this. Sometimes they will game popular Google search results to get you to click on a website under their control. And sometimes they will get a domain name that is similar to a popular one knowing that people sometimes misspell website names. For example, a scammer may have amzon.com to trap people trying to go to amazon.com.

Though not as common anymore, scammers still call people and say you have a virus but they can fix your virus. This isn't as common now because people have gotten wise to that scam and because of so many illegal robocallers people tend not to answer numbers they do not know. What is becoming more common is the scammers will now send you a text message instead of calling. But scammers will still call, so vigilance is still needed.

Scammers also still have much success with phishing emails. This is detailed below.

However it is done, the result is always the same: You are told you have a problem, usually but not always a virus or you have been hacked in some way, and that you should not turn off your computer but call immediately to get it resolved. Sometimes they claim to be Microsoft (they are not) and sometimes they claim to be Microsoft certified (they are not). Some will have sounds and a voice telling you that you have a problem. The really good ones know if you are using Windows or a Mac and adjust accordingly. Some of the newer ones know who your internet provider is to make it seem more legitimate. If you call the number, they will try to trick you into letting them take control of your computer. With very few exceptions, the scammers use legitimate programs to connect to your computer. Once they have access, they do a lot of nothing that looks like they are doing something. The bad ones purposefully sabotage your computer so that if you do not pay you won't be able to use your computer. The goal is always the same: to scare you into paying up. Some, once they have your credit card, use it to make more charges. But this is not common because they do not want the credit card companies to be alert to them. Plus, credit card companies can do a chargeback and get all their money back. Instead, they usually want you to pay by non-refundable means – wire transfer, gift cards, bitcoins, cash.

The fix is usually quite simple: Restart your computer, by force if necessary. You may have to restart more than once. Do not ever call the number. And avoid the last website you were on for at least 24 hours. If someone calls you, hang up on them. Or, put your phone down, walk away, and let them talk to the air. If you get a text message, immediately delete the message and report the number to your cell phone company's spam service. If you want to call about something, never ever call a number given on a website; always without exception call the number on your bill. Remember: scammers can create fake websites that look like the real ones to trap you.

Whatever you do, never ever let someone control your computer unless you know them face-to-face or unless you call the manufacturer from a number you are absolutely sure is the business's number.

The illegal robocaller scam

Most people don't know this, but in the United States all telemarketers must have a living, breathing person on the other end. Any recording for solicitation of any kind is illegal. Therefore, by definition any service the recording offers is a scam. A robocaller is something that automatically dials several numbers. This is one scam that does not always play on your fear or greed.

There are legal robocallers. Politicians can robocall you to death because any recording for political purposes is legal. They may annoy you, but political robocallers are not trying to get money from you. And besides, you must remember that rules that apply to everyone usually don't apply to politicians. Government agencies can also robocall you. Almost always they do this to inform you of something – school closing, amber alert, fugitive alert, boil water advisories, and other things like these. Certain businesses may also call and leave a recording if you opt-in. For example, your pharmacy may call you to inform you that your prescription is ready. In these instances, you are not asked to give up money or information so at worst it is just annoying and at best quite helpful.

Remember: the government will never ever call you about a legal problem. If you owe the IRS money, you are getting a certified letter or a sheriff deputy knocking on your door. The same is true for arrest warrants or any legal action.

Although the FTC has been trying to get phone companies to stop robocallers for years, little work has been done. The only thing the phone companies are working on now is to prevent phone number spoofing so that the number on your caller-id is the real number of the scammers. However, this will not stop the illegal robocallers because they can use cheap disposable numbers that you can get from legitimate services like Vonage. I can get a legal, North Carolina number for $6.12. These cheap and legal numbers use the internet to make a telephone call. With those numbers, you can be anywhere in the world, but probably India where there are enough English speakers to make it effective. The scammers work over people for a few weeks and then stop using that number to stay ahead of the government and call blocking services. (However, the government can eventually catch up to the scammers, because the money has to be routed through the United States somehow.)

Whatever you do, always hang up when you get an illegal solicitation recording. Doing anything else confirms your number to other illegal robocallers. If you have AT&T U-Verse, any VoIP phone service, Comcast, or Centurylink VoIP business then you can block robocallers using a service called NoMoRobo – www.nomorobo.com. You usually must activate the service through your online customer portal. If the number is on NoMoRobo's block list, it picks up after the first ring to filter out the call. If your internet is fast enough, I also recommend a landline phone service called Ooma, www.ooma.com. The premier service includes robocall blocking and it might save you money.

The fake prize scam

There are a few types of attacks: phishing and spear phishing. These attacks are based on how a person fishes or spear fishes. What you usually think of fishing is when a person puts some bait on a hook and does not know what will bite. A phishing attack is like that. A scammer throws out some bait but does not know what will bite. When you go spear fishing, you are targeting a specific fish. Once you see the fish you want, you catch it by throwing your spear into it. In the same way, with spear phishing, a person is being specifically targeted. The fake prize scam is a phishing attack, not a spear phishing attack.

The way this scam works is that you are told you won some money, but in order to claim it you need to pay a processing fee. A well-known variation is you are told that some rich person (such as a Nigerian prince) needs to move some money and he is willing to cut you in on a large portion of it if you give him some money. However it is worded, the tactic is the same: you have to pay some money to get more money. The tactic plays on your greed.

Some of these phishing scams will warn you about phishing attacks. This is an attempt to trick you because the scammers want you to trick you. The idea is to get you to think that scammers won't warn you about being scammed, therefore this is legitimate. As has been already stated, studies have shown that the more people who are aware of phishing scams the more likely they are to be duped.

Legitimate sweepstakes do not require money to receive a prize. This is why the legitimate ones say "no purchase necessary". You may have to jump through more hoops to enter without paying somehow, but you can win without paying. And do not be fooled: you are not someone a money launderer would contact, so you there is no Nigerian prince waiting to cut you in on a deal. If you get this scam by email, just delete it.

Brushing scam

For this scam, you are not the target. Amazon and other similar websites allow third parties to sell items through their website. The more they sell, the better they look to other people. Although Amazon is referred to below, this is not limited to Amazon. These same websites also allow you to post reviews of the product. People who actually bought the product on Amazon will have a notice beside the review saying "Verified Buyer".

Unethical scammer businesses will buy their own product, almost always something cheap and lightweight, from themselves using different Amazon account for each item and ship it to random people throughout the country. With that, the scammers will post a 5 star product

review and a 5 star seller review. The goal is to make the seller seem legitimate and to make the product seem like it is worth buying. The people being scammed are the ones who buy a sorry product thinking it is a good product.

If ever you received an item from Amazon, or a similar company, that you didn't order, first make sure none of your family or friends bought you anything as gift. If they didn't, then contact the company's brushing scam department or unwanted package department. This will help Amazon, Newegg, Alibaba, and so on remove the bad actors from selling on their website.

The bank charge verification scam

This is a type of phishing scam that is complicated and long. But very effective. It takes two stages. This is done to make you lower your defenses.

The first stage is the prep work for the scammer. Currently, they are sending out text messages claiming to be your bank. To make this effective, the scammers already know who you bank is. The text message claims there is a large charge and you are asked to confirm the charge by replying to the text message. If you reply at all, the scammers know you are likely to be manipulated further. The problem for you is that banks really do send out text messages asking you to confirm large checks.

If you reply to that text message, a scammer will then call you. The really good ones, while still in India, have an American accent. They don't ask for your password or any information that would quickly clue you in on the scam. The scammer walks you through an entire process to help "reverse the charges". What the scammers are doing is working to gain control over your account. Eventually, you will be asked to transfer or send the money to yourself. In reality, you are sending money to an account that the scammers have just taken over.

If there is any doubt of a purchase, it is best not to reply to a text message. Instead, you should call your bank directly, with a number you know to be valid. And never ever transfer money between accounts over the phone; always do this in person at your local bank.

The lost money/better discount/overpayment refund scam

This is not the refund scam, where you are asked to refund some illegally obtained items to a store. This scam takes various methods, but the principle is the same: someone claims that you are owed money or that you can get a better deal on your service and that person can help you obtain that information. For instance, a person or email or text message tells you that you were scammed and then offers to help you get your money back. Another example, a person claims that Microsoft, Apple, Amazon, or similar incorrectly charged you or incorrectly charged you too much and that this person can help you get a refund. Another example, a person claims to be from your cable provider – and the really good ones know who that is – and that they can get you a better deal.

Here is an example: You receive a call claiming you were accidently charged a large amount, an amount that always ends 99. For example, $399. Because you were accidently charged, or overcharged, this amount, this person is authorized to get your money back. Because of the inconvenience, you will be refunded $1 more. The scammer then asks for and gets permission

to access your computer, he asks you to go to some website or your bank's website so that the refund can be processed. You are asked to enter the amount, in this example $400. But before the scammer presses submit, an extra 0 just so happens to appear. "Oh no!" says the scammer. Instead of refunding you $400, you are now being refunded $4000. This person is now in big big trouble. But you can keep from being fired, just buy several gift cards to make up the difference, in this example that would be $3600 in gift cards.

The tell-tale sign of this scam is that you are offered to get money back or save money. This scam plays on the natural desire that everybody wants more money. More than likely, the person will ask for some non-refundable payment, such as gift cards or a wire transfer. And sometimes the person will ask for your Amazon account information, your bank information, some personal information, or something similar. Usually, but not always, the person will not ask for credit card information because the credit card company can refund the money.

Never ever let someone control your computer to help you recover money or save money. Never give your credit card number, bank account information, or social security to someone who calls you, text messages you, or emails you. And never ever send a wire transfer, gift cards, pre-paid cards, or bitcoins to someone you wouldn't trust with the keys to your house. Never ever call the telephone number provided in an unsolicited message, even if it is a toll-free number. Always – *always* – call the number on your last bill.

The refund scam

This scam is a problem for businesses. In this scam, a person refunds something that is not eligible for a refund. To cover their tracks better, sometimes a scammer will ask you to refund some items for someone else. The item could be illegally obtained, damaged, and sometimes the item being returned is a lot of nothing that weighs the exact same as the item purchased. This can also affect customers. In one instance, a person bought a computer from Wal-Mart, stripped the hard drive, memory, and processor and then returned the computer. Wal-Mart then sold the computer to someone else. Wal-Mart only lost a little money; the customer who bought the computer lost a lot of money. Amazon takes and refunds so many orders that some scammers will buy something from Amazon, take the item out, put something in the box that weighs the same, and then return the item. Because Amazon is so big it may take months before they discover they have been scammed.

Refund fraud is a very serious problem for businesses. To combat this scam, businesses track refunds closely. This is why you are now limited to the number of refunds a business will accept from you in a year.

Do not refund anything for people you do not know very well.

The strange email from your friends scam

Someone you know sends you an email. It seems strange because it is not their style. It usually does not use your name. But it does have something like this in the message: "I was thinking of you when I saw this link." And then it has a strange link to a web page. The email does not use a person's email signature (if he has one). In this scam, your friend has had their email password hacked.

Hackers and scammers love to crack email passwords. Once in, they might discover who your bank is and then they can potentially, with enough time and patience, hack your bank account and siphon money. Or they crack into something else you need to keep private. But that is a lot of work. Usually, once the password is cracked they send out emails to your contact list in your name in an attempt to get you to click on a web page. If you do, the web page might attempt to plant some malicious software on your computer, or it might display the fake security alert scam, or it might use your browser to keep clicking on ads in which the scammer gets paid per click. The last scam is known as click fraud, and the scammed victim is an advertiser.

If you ever get one of these emails, reply to your friend and let him know he has been hacked. Tell him to change his password immediately. Also tell him that if any financial information was sent to that email address then he needs to change those passwords too, just to be safe. Everyone, including your friends, should use a different password for each important website and a different one than that for email. That way, if hackers get one password then they only get that one, and not all your passwords. Keep a paper notebook with your passwords so you will remember them. Also, be sure to use fake answers to security questions and write the fake answers down in your notebook. In this way if someone knows anything about you they will not be able to correctly guess the security question and thus not be unable to reset your password.

The relative or friend in trouble scam

This scam can take a few forms. You get a call or email from someone claiming to be a relative in trouble and they need money now. Usually this scam preys on grandparents or the elderly because age slows down mental abilities. In a common form, someone will claim to be a grandchild in trouble. Another form is when someone builds up a relationship with you over time, usually but not always a romantic one, and then suddenly that person needs money to get out of trouble. Sometimes, however, the friend just needs money to buy something. Whatever form it takes, the result is the same: to play on your emotions to get you to send money.

Do not send money to anyone without talking to your family. If someone calls claiming to be a relative, ask for a name. But be warned, some of the really good scammers do know your family and personal life well. Never ever under any circumstances send anyone a large number of gift cards. Only send a money order to someone you know face-to-face and have known for many years and to an address you know for certain to be the person’s address. As for the ones playing the long con, remember the basic rule: Never send money to anyone you do not see face-to-face for long periods of time and never send money to anyone you would not trust with the keys to your house.

Here is a good idea if you have family that might be susceptible to this scam: Have a safe word. Make everyone in the family remember a safe word. This may require a lot of patience if a person has already lost mental abilities. Above all else, make sure the safe is never ever posted anywhere on the internet. Whenever someone in the family claims to be in trouble, make them use the safe word. Wrong safe word means a scam.

The verification scam

This scam comes in many forms. In one method, someone is claiming they require some personal information for verification purposes. They could impersonate your phone company, another company you have an account with, the IRS, the FBI, or anybody else. Quite often, it is a call claiming to be from your phone company, Apple, or Microsoft. You may get an email that looks like it is from the real entity or you may get a call with a spoofed caller-id number from the legitimate company. Sometimes you are told if you do not take action in providing the information, your service will be cut off or you will be arrested. The purpose of this scam is to get your personal information that can be later used for identity theft.

Another form of this scam is by a phishing email. You get an email claiming something needs to be verified. Or you have to provide more information to complete an order or something else where you have to provide some personal information or a credit card number. Sometimes the email link is random letters and numbers. But the more successful ones have a link with the company's name in it. For example, if you get an email claiming you won a $100 Amazon gift card, the link in the email could be for a website amazon-gift-cards.com. That is a hypothetical example to show you how you are tricked. Also, websites can now use differ rent alphabets in websites. The Cyrillic letter 'p' looks exactly like the modern Latin letter 'p'. So, scammers will mix and match alphabets to get a website that looks like the real thing to you. As an example, this hypothetical link uses both Latin and Cyrillic letters: amazon.com. The vowels are Cyrillic and the consonants are Latin. A computer knows which is which, but to your eyes it looks exactly the same.

A third form of this scam is you get a call or email claiming to be something you are associated with. This could be your company, your university, your children's school, or similar. You are asked some kind of personal information. Sometimes the link in the email also has that institution in it somehow.

If a government agency needs to verify something with you, you will never ever get a call or email; you will get a certified letter in the mail or a sheriff deputy at your door. If a company you have dealings with needs some information from you, they will also send a letter. There are no legitimate organizations that will call or email you if they need information. And even if you get a letter claiming you need to provide information it is best to go to that organization's website direct or the number on your last bill and call the number provided there, and not the number provided in the letter.

The fake renewal scam

In this scam, you receive an email claiming you need to renew a product. Or the email claims a product has been renewed. This is a regular phishing email scam. The purpose is to make you afraid: afraid that your security has expired or afraid that you have been charged. The goal is to get you to call them. The fake tech support scam often has a charge under $1000. The goal of those is to make you think you are getting something of value. These scams may try to steal even larger amounts of money.

If ever there is a doubt, *do not* call the phone number in the email. Instead, contact the company directly using the contact information on their website or on your paper bill. Always double-check the phone number you are calling. I do this by putting the number in Google in this way: 888-000-0000 or 888000000. No matter who you call, never give out your banking or personal information.

See the section at the end of phishing email scam examples.

I would also recommend you report the email as a phishing or spam email if your email provider lets you do that.

The email claiming to have hacked you

You get an email which claims to have successfully hacked your computer or phone. The email claims they have sensitive information or photos. For example, many times it says they have proof you have been on pornographic websites. You are asked to pay a fee or else they will release the information.

This is just a phishing attack. The scammers didn't hack your computer or phone; they don't have any information on you. Just delete the email and sleep well because your files, information, or browsing habits are safe.

The blackmail scam

This scam takes many forms, of course. What is becoming more common is you get an email claiming you have been hacked or have some malicious software on your computer. The blackmailers will provide a password you actually used. The email concludes by asking you to pay a fee in non-refundable bitcoins.

More than likely, you were not hacked. Almost always, the blackmailer bought a list of email addresses and passwords from a hacked internet server. To help isolate which service, simply go to www.haveibeenpwned.com and put your email address in.

What you need to do is change the password on every website that uses the password the blackmailer gave. And be sure to change the password to your email as well. Once that is done, consider changing the password to all websites. I like to keep an Excel spreadsheet, or paper notebook, of websites and the passwords I used. I also put fake security answers for the security questions and that in my notes. When all that is done, sleep well at night.

The FBI, IRS, or similar has a warrant for your arrest scam

The really good variations of this scam know a lot about your personal information to make the scammers seem to be legitimate.

Like many scams, this scam is designed to scare you so that you do not think straight. Just like the verification scam, you may get an email or call that looks legitimate. The way the scam works is by saying some government agency has a warrant for your arrest and you need to pay up right now to resolve it. Many times, you are asked to send pre-paid gift cards, wire transfers, or the virtual currency bitcoin to resolve the issue. This is because once those are sent, there is

no way of getting your money back. With a credit card, you can dispute the charges or do a chargeback and the scammer can be out of his money. With the other, you have no such protections.

A twist on this scam is the call or email claiming to be someone from the FBI or IRS or similar claiming to be someone in the agency with a position of authority. This person also claims to have access to your criminal file, name, address, phone number, and other personal information. For a bribe they will quietly claim to destroy your criminal file. Similar to the hacked email scam, sometimes they say they have proof of child pornography or pedophilia. It might be some other very serious and embarrassing felony.

Another twist to this scam is someone claims to be the social security administration, and the caller-id will display the actual social security number. The scammer will claim that you need to verify your account to keep the benefits going. If successful, another scammer may call you pretending to be from the FBI and tell you that you were scammed. For a fee, the FBI would go after the scammer.

If any government agency needs you for any reason, you are getting a certified letter in the mail or a letter hand delivered by the sheriff. You will never ever get a phone call or an email about this. While it is possible that government agents are susceptible to bribes, the chances that someone is actually willing to be bribed to go after you is very low. And besides, when the FBI or IRS arrests you, they tend to seize assets obtained illegally. Why would someone accept a bribe with so much oversight and when they can legally take it after a conviction? Just destroy the email or ignore the phone call.

The one ring phone scam

You get a call, usually in the middle of the night, and the phone rings only once. Sometimes, you are called several times with just one ring. Your natural instinct is to think that if someone is calling in the middle of the night, it must be an emergency with someone you know. And if you are awoken from your sleep, the chances are good you are not thinking clearly too. The purpose of this scam is to get you to call back. The number on the caller-id is an international toll number. By calling the number you will be billed for every minute you are on the line. Therefore, it is in the scammers' financial interests to keep you on the line as long as possible.

Never ever without exception call someone back from an unknown number who does not leave a message. Make sure your friends and family members know that they should leave a message so that you know it is legitimate. You can also set your cell phone up so that only numbers in your contact list will ring between certain hours of the day.

You can stop this scam by asking your phone provider to block international calls. Unless you know someone in a foreign country or need to make or receive calls with your cell phone in a foreign country, you won't need this feature. And even if those situations apply, you can make free calls using apps like Google Hangouts, Vibre, and many more. These only need a Wi-Fi connection, an account with that service, and both people using the app. Alternatively, you can unblock international calls only when needed. Some cell phones now support Wi-Fi calling. With this feature, you can make calls anywhere in the world without being charged a cell phone

roaming fee as long as you are connected to Wi-Fi; you will still be charged the other fees such as toll or international dialing. Your friends or family can also use that feature to call you from outside the country without a strange number or a special app.

This scam works because several countries use the same phone numbering system as the United States. These include all US territories and almost every Caribbean country except Bonaire, Cuba, Curaçao, Guadeloupe, Haiti, Martinique, Saba, Saint Barthélemy, Saint Martin (but not Sint Maarten), and Sint Eustatius. The scammers will quite often use a number from one of the Caribbean countries that use the same numbering system as the US. You likely do not know every American or Canadian area code, so you will not know which area code is from a Caribbean country.

The boss needs information scam

This is a type of spear phishing attack. Scammers, or someone worse, are looking to get internal company documents. So they pretend to be your boss, maybe even impersonating his email, and asking you to send some important documents. In some cases, they have cracked the boss's email so that once you send it to him, they get it too. In other cases, the reply-to settings on an email are to an email address under their control. The purpose is for industrial espionage, access to your banking information, identity theft, or sabotage.

If your boss ever asks for confidential and sensitive documents, be sure to call him first. And call with a number you know to be him. Also alert your company's IT department right away, regardless of whether it was legitimate or not.

The ransomware scam

Now this one is especially bad. Somehow or some way your company picks up some malicious software. Quietly in the background, it encrypts your data because it is holding them for ransom. The really good ones do this slowly so you are less likely to notice. And the best of the best also encrypt your backups so that you cannot recover. But those are rare. Once it encrypts as many files as it can get away with, it gives you a message telling you what it did and then deletes itself so that you will have a hard time recovering the files on your own. Usually you have a short time to pay up, or else you will not be able to get the recovery method. The most profitable ones base their fee on how many files are encrypted. What is worse, the payment is never by credit card but by virtual currency (i.e. bitcoin), gift cards, or wire transfers. The latter two are impossible to recover any scammed money, the former is very difficult and would require federal government action.

Most ransomware scams are targeted to business because they are the ones likely to pay. But it is still possible that individuals will get ransomware.

This scam works because most people do not backup. What is worse, stupid Microsoft took away the full backup program in Windows. Probably because they want you to buy one from the Windows store and thus they get a percentage of the software sale. So now you are left with important documents or pictures that can only be recovered if you pay up.

The simple solution is to have a backup. Although Windows no longer has a proper backup program, it does allow you to make copies of files. It is called file history. That is probably good enough. A USB external hard drive is not that expensive anymore. The cheapest one is more than adequate for a copy of your files. With that extra copy, you can be safe from this scam.

The unusual order scam

This scam affects businesses, usually small businesses. You will receive a call or an email from someone who wants to place an unusually large order. Or some other strange order. As a small business, you like large orders. For instance, a computer repair business may be asked to order many laptops. You are given a credit card, likely a stolen credit card but definitely an invalid one, and it will process successfully. Or you may be given an invalid check that will deposit successfully but will bounce a few days later. You will then be asked to ship the product to them or use a shipping service that is not FedEx or UPS or USPS. If you are asked to use a shipping service, you will call a number given and you will pay by credit card for shipping. But nobody will ever come and pick up the packages. Regardless, you never deal with anyone face-to-face.

Because an invalid credit card or check was given to you, in a few days you will lose the money paid. If you ship the product to the scammers, you are now out of the product with no way to get it back. If the scammers ask you to use a special shipping company, you will actually be paying the scammers direct because that special shipping company is just a bogus one under their control.

Be wary of someone you have no prior business relation to asking for large unsolicited orders. Check the email address. Large businesses will not use free email accounts like Gmail or AOL or Outlook.com; they will use a company website. And if the email is a company one (i.e. bob@bobscompany.com), research the company. I would even call the company using contact information on their website and Google the company to make sure it is legitimate. For any unusual order, ask for the phone number on the credit card and call to confirm the credit card is valid. Research the phone number to make sure it is a valid credit card company; *do not call* before researching the number. Once you are sure the phone number is legit, call the company and ask about this card. Make sure you give the credit card company the address given to you for shipping. If given a check, require a waiting period and go to your bank or the bank of the check if possible and verify it is a valid check. Always require a non-refundable deposit.

Here is an example of this scam. In red lettering are my comments showing how you can identify this scam. I am providing the scammer's email address because by the time you read this, it will be deactivated.

```
From: David Serano <davidentm02@gmail.com>
Date: Mon, 3 Jun 2019 18:10:10 +0100
Subject: Laptop order
To: --@techs-on-call.biz
Hello Sir/Madam
          This David Serrano from Kirkland Shipping,We
looking for laptop computers to purchase for our new
business branch and want to know if you have them available
```

in stock or can either custom order them for us.We also do have specifications we would like the computers to come with and also if you can tell us how much a laptop with these specifications is going to cost for plus tax...Here are the specifications below ,

(First, any professional company would not have so many grammatical errors. Second, any large business would already have an account with Dell, HP, or Lenovo and so wouldn't want to pay your markup to get what they can get. Third, why would a large business use a Gmail email address and not the email address of their company? In this scam example, why isn't the email from @kirklandshipping.com or something like that?)

An i7 Core Processor

16gb of Memory

1tb of Hard drive or 512 SSD

Screen Size can either be 13' , 14' or 15.6'

Must come with a Touch Screen and a backlight Keyboard

Either a windows 10 Home premium or Professional

Brands can either be Dell , Hp or Lenovo

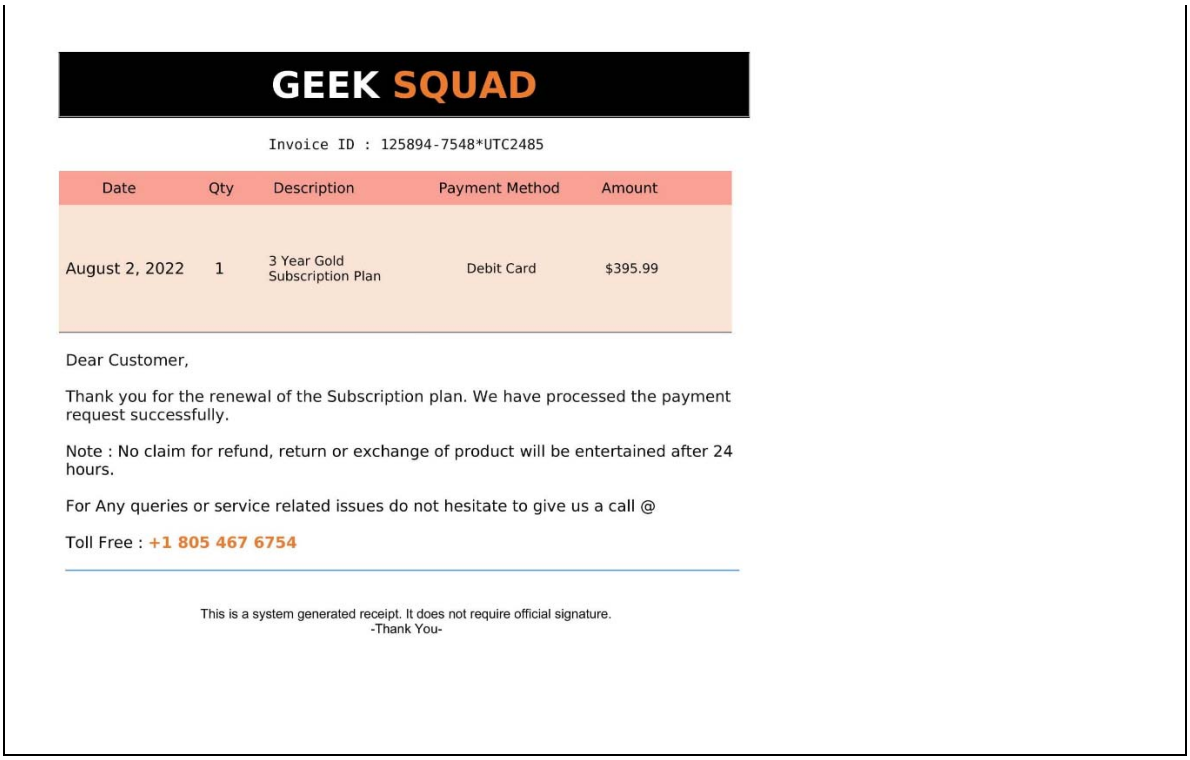
NB : Also advise me if you do take credit card payment , Thank You !

(The credit card they will give you will be stolen or invalid. Because of processing delays, the transaction will fail after you pay their bogus shipping courier or after you ship the product you paid for to them unless you are a real slowpoke.)

Phishing email scam examples

Renewal phishing email scam example. I have seen variations of this email using McAfee and Norton antivirus. The company is different; the template is the same.

From: "Noura" <n8553894@gmail.com>
To: billing@geeksquad.com
Sent: ----
Subject: Invoice # 579062447



GEEK SQUAD

Invoice ID : 125894-7548*UTC2485

Date	Qty	Description	Payment Method	Amount
August 2, 2022	1	3 Year Gold Subscription Plan	Debit Card	$395.99

Dear Customer,

Thank you for the renewal of the Subscription plan. We have processed the payment request successfully.

Note : No claim for refund, return or exchange of product will be entertained after 24 hours.

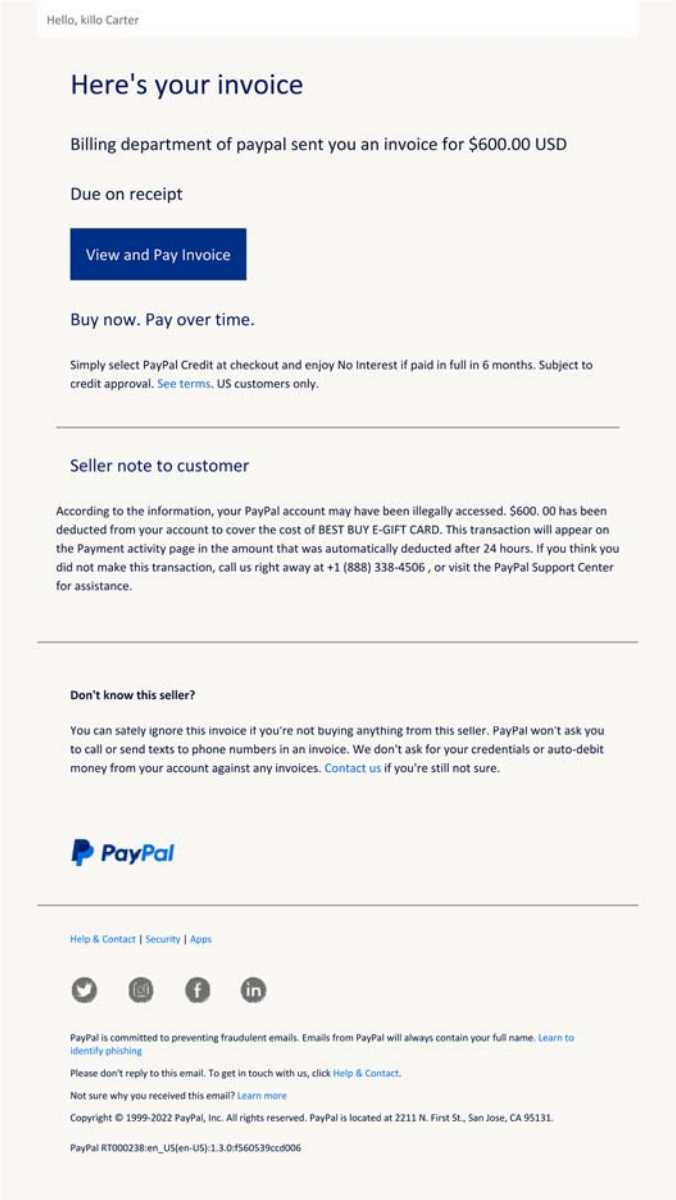
For Any queries or service related issues do not hesitate to give us a call @

Toll Free : +1 805 467 6754

This is a system generated receipt. It does not require official signature.
-Thank You-

If you notice carefully, the content of the email above is a picture. This is done to bypass spam filters. How can you tell it is a picture file? Try to highlight any of the words in the invoice. You can't do it. Now try to highlight any word in this paragraph. You can do it. There are a few other tells in the email. First, notice carefully *who* this scam email is from. It is not from @geeksquad.com or @bestbuy.com. Rather, it is from a free and disposable gmail email address. This is probably a legitimate email, at least for a few days, to try and bypass spam filters. Second, notice carefully who this email was sent to. It does not use that person's real email address, but it is listed as billing@geeksquad.com. This is another attempt to bypass spam filters. Third, notice that the payment method said "Debit Card" and not "Visa ending in …" Legitimate bills tell you which card was used so that you know which payment was used. Scammers want to send this email to a many people as possible. A specific card would allow people to check, and scammers don't want you checking anything.

Here is a difficult one. See if you can spot the scam. I converted the entire email to a picture so that you can see what it originally looked like in Microsoft Outlook.



Hello, killo Carter

Here's your invoice

Billing department of paypal sent you an invoice for $600.00 USD

Due on receipt

View and Pay Invoice

Buy now. Pay over time.

Simply select PayPal Credit at checkout and enjoy No Interest if paid in full in 6 months. Subject to credit approval. See terms. US customers only.

Seller note to customer

According to the information, your PayPal account may have been illegally accessed. $600. 00 has been deducted from your account to cover the cost of BEST BUY E-GIFT CARD. This transaction will appear on the Payment activity page in the amount that was automatically deducted after 24 hours. If you think you did not make this transaction, call us right away at +1 (888) 338-4506 , or visit the PayPal Support Center for assistance.

Don't know this seller?

You can safely ignore this invoice if you're not buying anything from this seller. PayPal won't ask you to call or send texts to phone numbers in an invoice. We don't ask for your credentials or auto-debit money from your account against any invoices. Contact us if you're still not sure.

PayPal

Help & Contact | Security | Apps

PayPal is committed to preventing fraudulent emails. Emails from PayPal will always contain your full name. Learn to identify phishing

Please don't reply to this email. To get in touch with us, click Help & Contact.

Not sure why you received this email? Learn more

Copyright © 1999-2022 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

PayPal RT000238:en_US(en-US):1.3.0:f560539ccd006

There are 3 tells that this email is a scam. First, the name is not you and is not capitalized correctly. Who is "killo Carter"? What is the k lower-case? Second, notice the grammar in the sentence below “Here’s your invoice”. To be correct English, the sentence should begin with “The billing department …”. In that sentence, the word “the” is left off. Also, Paypal should be capitalized in that sentence. Third, the phone number in the email is *not* a Paypal number. I checked.

The email used several things in attempt to lower your defenses. The links in the email went to Paypal’s website. The email was said to be from service@paypal.com. And it was warning you against scams. Some scammers do that because people wouldn’t think a scammer would warn them about being scammed.

If you receive a similar email, always *always* ***ALWAYS*** go to the website directly and call the number there or call the number of your paper invoice. Never ever, without exception, call a number provided in an email.

---

[i] Phishing in an Academic Community: A Study of User Susceptibility and Behavior (https://arxiv.org/pdf/1811.06078.pdf)

[ii] Robocall bagmen admit they collected millions of dollars from victims scammed by bogus IRS officials, lenders (https://www.theregister.com/2021/02/24/robocall_scam_bagmen/)