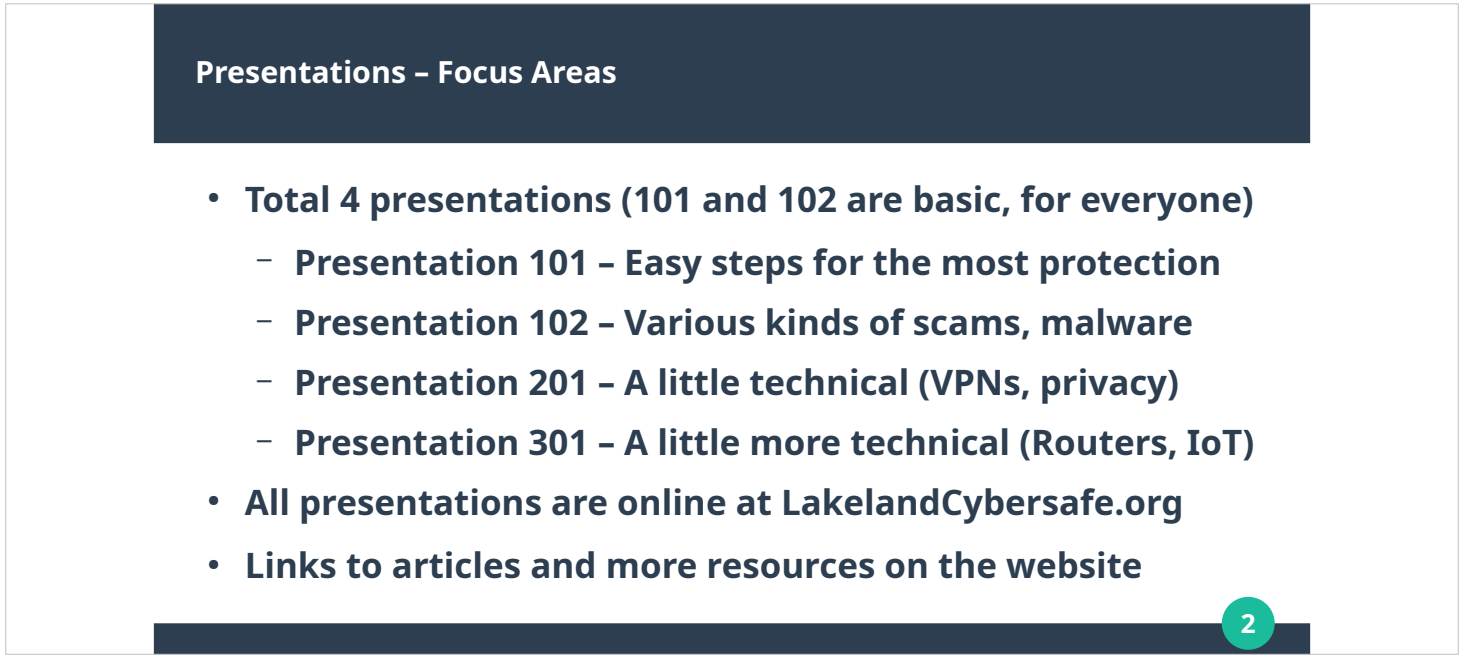
Thank you for showing up to this presentation on cybersafety. It may not be the most fun topic to discuss but it's an important one that could save you time and money and help you become more confident as you navigate the Internet. Many of the scams we will discuss have been around before the recent injection of AI into the public sphere, but what's different now is that AI has turbo-charged the scammer's toolbox.

AI has enabled scammers to become more efficient and dangerous and the scamming industry has become highly organized. What used to take a scammer some amount of skill and computer knowledge is now easily done by asking AI on a smartphone. So it's all the more timely now for us all to learn the fundamentals of cybersafety so we can identify and protect ourselves from a scam in progress.

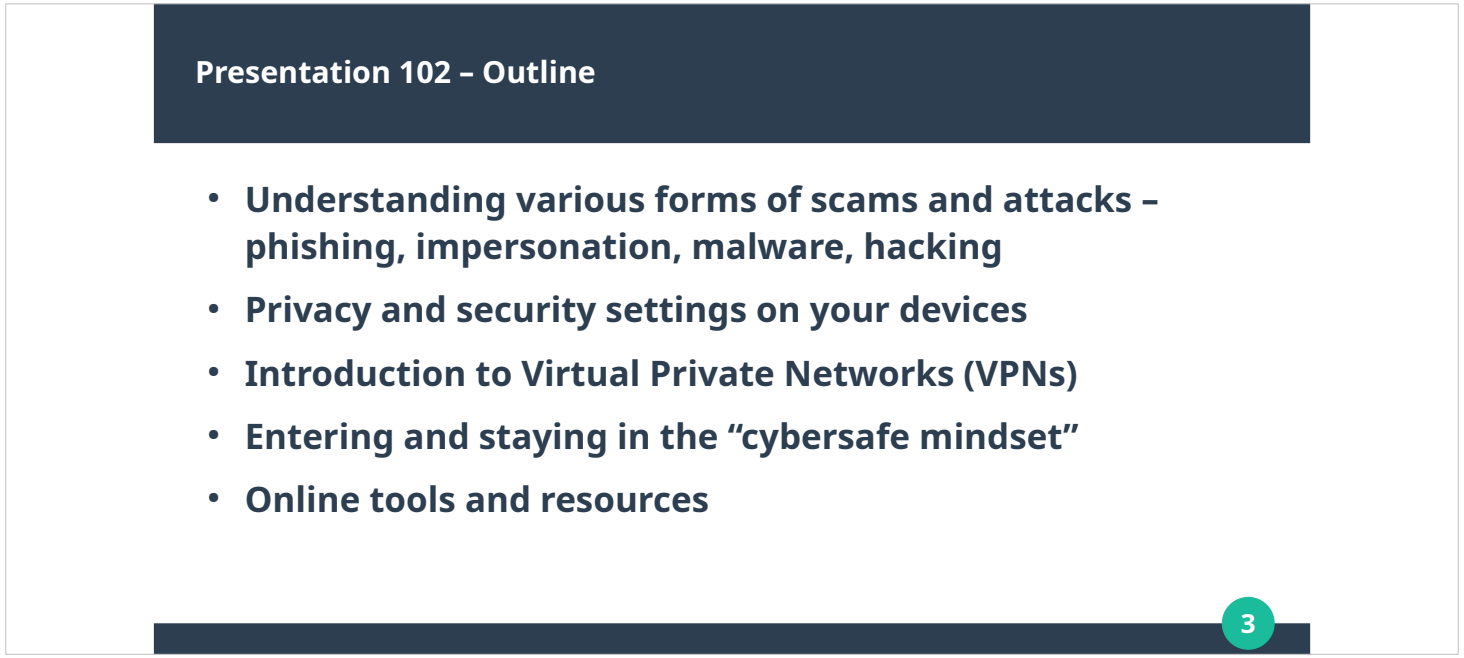


There are a total of 4 presentations. The first two are basic and are meant for everyone. If you use the Internet, check email, watch Netflix or shop online, you already have the skills to understand everything in the first two presentations. This presentation is the second – presentation 102, and focuses on various types of scams so you can become aware of what's out there and acquire the skills to identify what might be a scam attempt and protect yourself from it.

If you haven't attended the first presentation, you can watch it online at lakelandcybersafe.org. Among other things, it shows some practical steps you can take to protect yourself from identity theft, such as locking down your credit reports.

The third presentation in the series is slightly technical but still accessible to those of you who are a little computer savvy. We discuss why privacy is important and how it relates to security. The fourth presentation is about routers and other more technical measures.

Visit lakelandcybersafe.org for all the presentations, articles and more resources.



In this presentation, we’re going to look at various kinds of scams and fraud, like, phishing, impersonation, malware and outright hacking.

It’s about awareness but it’s also about knowing how to get to the right settings on your phones and computers to make them more secure.

We briefly look at what Virtual Private Networks are but really get into them only in presentation 201.

Finally we talk about what a “cybersafe mindset” is, how to develop it and how to stay in it.

There is a sizable list of cybersafety resources online and we look at some of them so you can walk away with some new knowledge from the presentation itself but also continue learning more on your own.

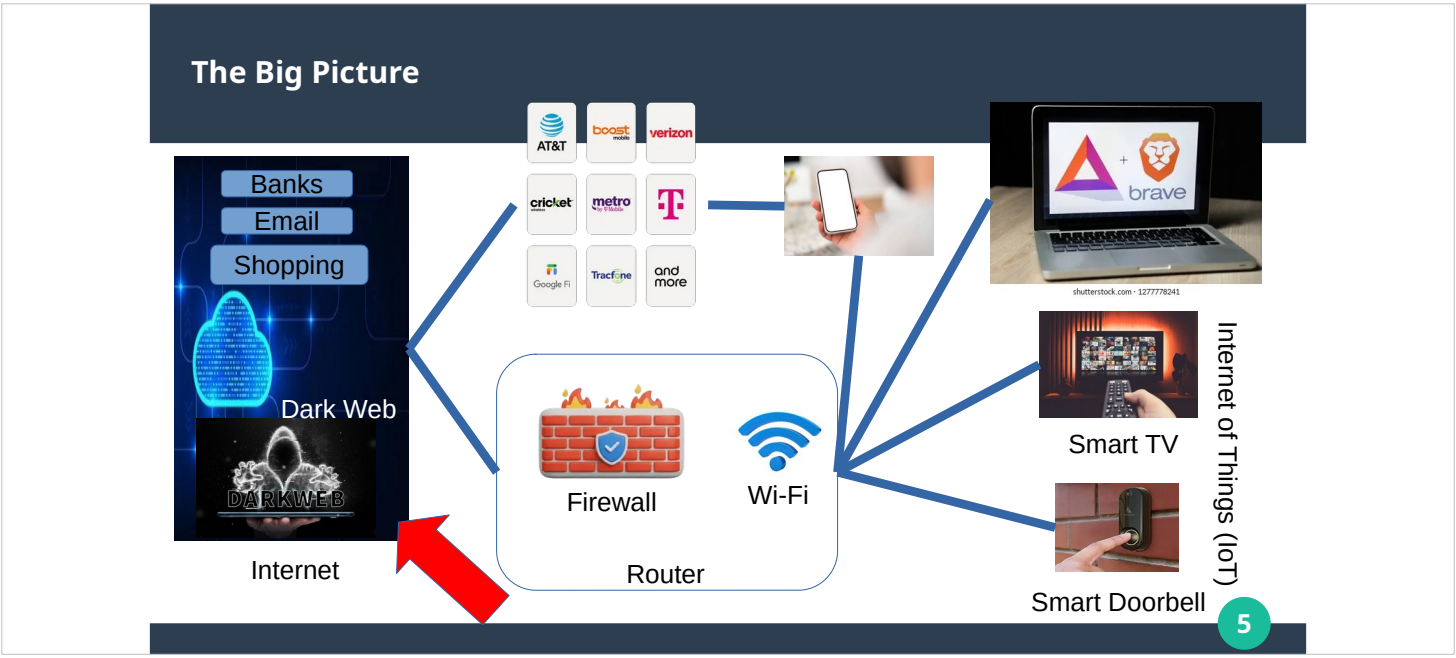
Questions?

- **Please feel free to interrupt at any time to ask questions!**
- **It's not a lecture. Let's make it lively and interactive!**
- **I'll be around after the presentation for more questions**

4

Let's make this a discussion instead of a lecture. Stop me anytime to ask a question, or to ask me to repeat what I have said. There are no dumb questions. If you have a question, it's likely that others also have the same question so you will be helping others too.

I will be here for a while after the presentation too in case you have any lingering questions.



We looked at this picture in presentation 101. It's a typical home Internet setup. You have the Internet on the left, and the devices on the right, and in between is the router that connects the devices to the Internet. In the case of the smartphone, when we are not home, we connect to the Internet through the cellular network.

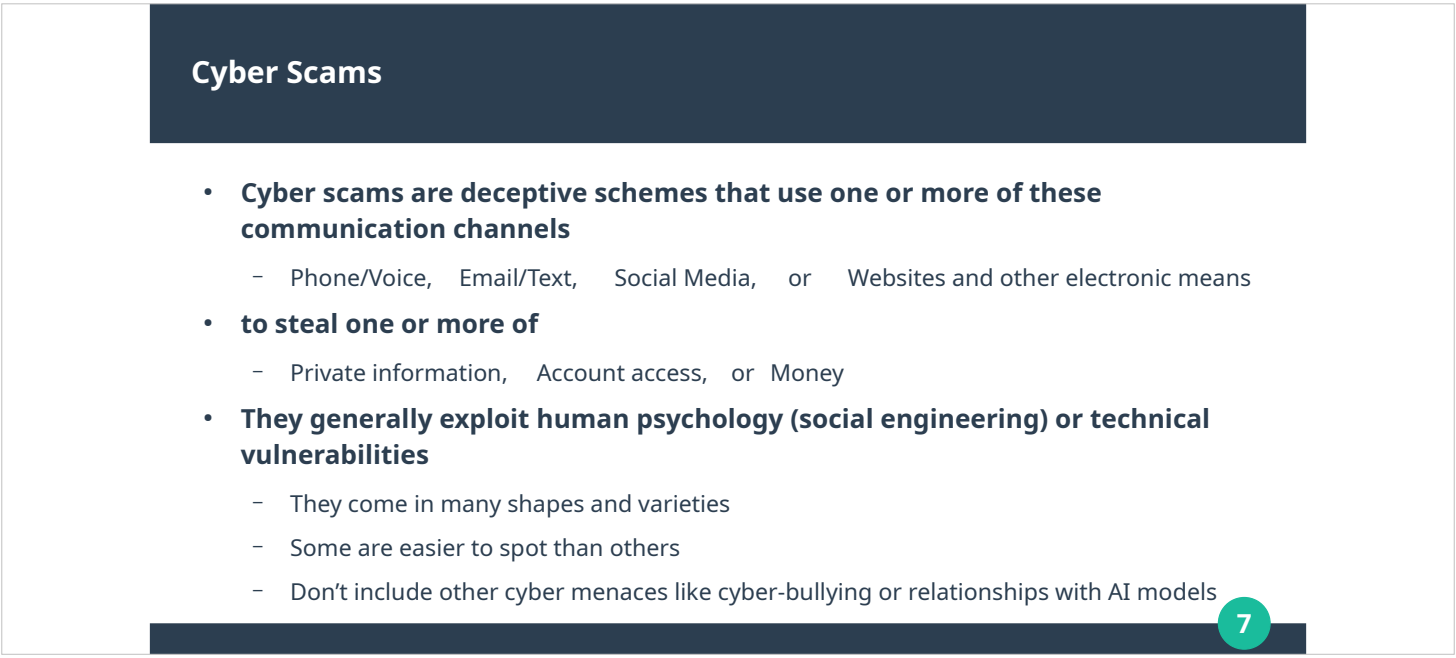
We're going to mostly continue looking at the Internet part of the picture in this presentation, but we will touch upon the devices later on, and what we can do to protect ourselves from the darker parts of the Internet which is where scams originate from.

As we saw in the first presentation, the part of the Internet called the dark web has a lot of private information for sale – our names, phone numbers, addresses, social security numbers and many other details that are used by scammers to target us. Not all scams originate from the dark web. Many are run-of-the-mill operations that prey on human psychology and don't need much technical expertise. In all cases, the more we know the anatomy of common scams, the better prepared we are.

A Typical Call Center(?)

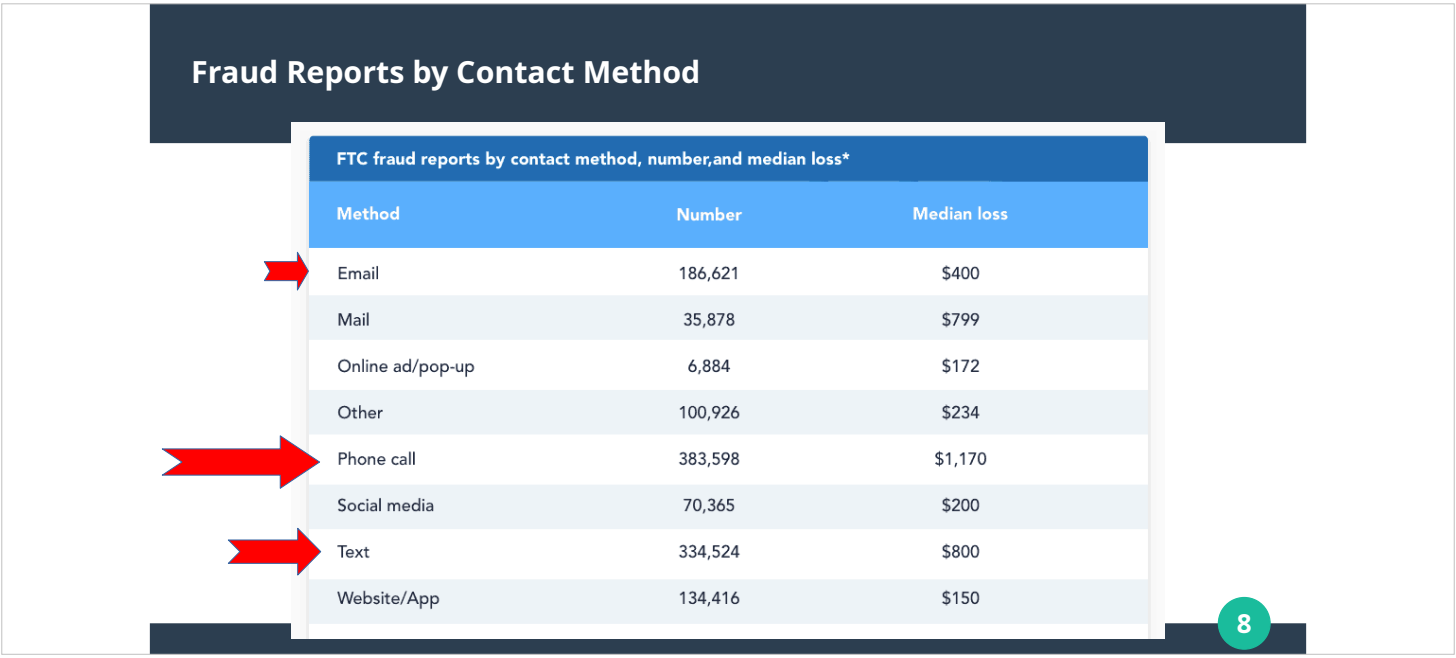
Take a guess as to what this is! It certainly looks like a regular office on any Monday morning with people busy at their desks making sales calls or helping customers. But it's actually a scam operation based in a city called Lahore in Pakistan. Not to pick on Pakistan, scam call centers like this exist all over the world in almost all countries targeting both residents of their own countries as well as foreigners. Some operations in countries like India, Pakistan, Bangladesh, Nigeria, Ukraine do specialize in targeting Westerners because English is a common language in these countries.

Americans are used to talking to customer service agents with an accent because large companies in America have outsourced their customer service to countries like India over the last two decades. So it's become increasingly difficult to identify scammers for who they are. However, there are several tell-tale signs and patterns that when we become aware of, we can catch them in the act.



What is a cyber scam? Cyber scams are deceptive schemes that use one of these communication channels: phone, email, social media like Facebook, or websites and are designed to steal either private personal information, account credentials like usernames and passwords or money. At the end of the day, the scammer wants our money. Stealing personal information is a step in that direction.

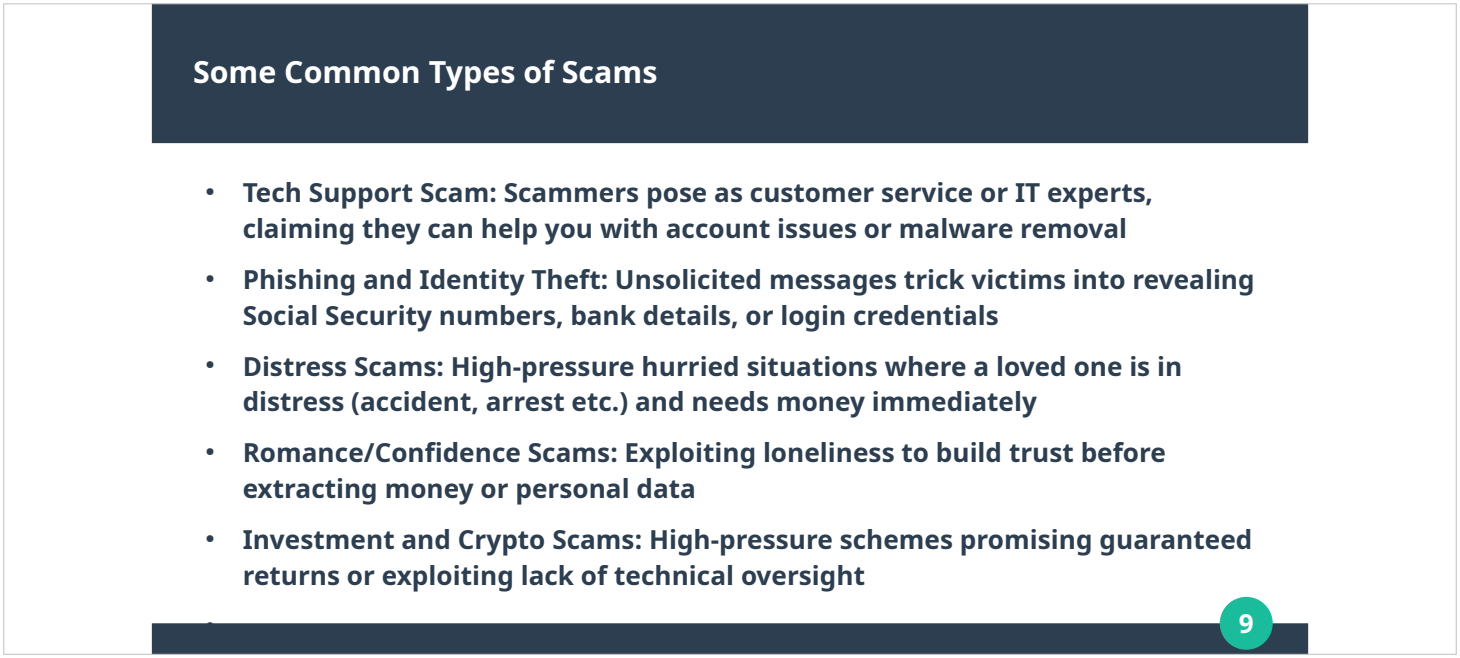
While technology is used at every step of a scam, it is generally human psychology that is the weak link in the chain. It's about building trust and exploiting the trust when the opportunity arises. It is for this reason that much of cybersafety comes down to awareness and developing the sixth sense that alerts us and says, "hey, something looks fishy here". The Cybersecurity industry that helps large companies stay secure also points out this fact: despite the billions of dollars companies spend on protecting themselves, it is typically a single distracted employee who inadvertently and unwittingly exposes the entire company to an attack.



We saw this slide in the last presentation but it's here again to remind us of the top three ways that scammers contact us:

Number one is phone call. Two is text and three is email. There is a reason why the trend goes this way. A phone call is personal, it is easier to build trust quickly and it's easier to create a sense of urgency which is a critical component of many scams. A text message is also suitable to create trust though not as personal as a phone call. Scammers often text us from a phone number with the same area code as ours, so it looks local and doesn't raise our suspicions. The advantage with texts is the scammer can send hundreds of them at the same time.

This advantage carries over further with email. It's easy and cheap to send thousands of emails and although they are not as personal as phone calls, they can still create that sense of trust and urgency for us to take the next step – which is to respond to the email in some way. When we make contact with a scammer and engage further, we risk giving up more personal information at the very least.



Let's now look at some common types of scams. We have tech support scams where scammers pose as technical experts or customer service agents. The picture we saw earlier was of a tech support scam call center. They pose as employees of Verizon and direct the victim to log in into a fake website that looks like the real Verizon site, but one they set up.

Then we have phishing scams which we will go deeper into. Think of phishing as fishing for your private personal information.

Distress scams are highly exploitative and create an immediate sense of urgency where a loved one is in an emergency.

Romance scams have been around for a long time but the Internet and social media have made it far easier than before to pull them of.

Investment scams have also been around but the anonymity offered by the Internet has made them more effective. Fake reviews and recommendations can be easily generated.

Many scams have elements from one or more of the above. For example, a scammer poses as a legitimate potential romantic partner, extracts information (phishing) and asks you to invest in a crypto scheme after a few months of building trust (investment scam).

Oh no, my computer crashed! It says, “Windows Defender Alert”. There’s a virus!

I might have to call Microsoft at this number now. Sorry everyone, I didn’t expect this to happen.

Well, if you see a screen like this, it is natural to be alarmed momentarily. Pause and take a breath.

It’s a tech support scam. Somehow, a scammer got us staring at a scary blue screen. It could be a browser pop-up or a virus they may have downloaded onto our computer but either way, they are waiting for us to take the next step and call that number they show on the screen.

DO NOT PANIC!

When a scammer gets a call, they can do any number of things. They can direct the victim to a fake website where they capture the username and password. They can ask the victim to download a program to their computer. They can ask for the one-time-password (OTP) to access an account that the scammer is attempting to hack into. They can ask for credit card information for payment for virus removal services. The possibilities are numerous.

Scammers also call you directly sometimes from a spoofed number. We get into spoofing in the next slide.

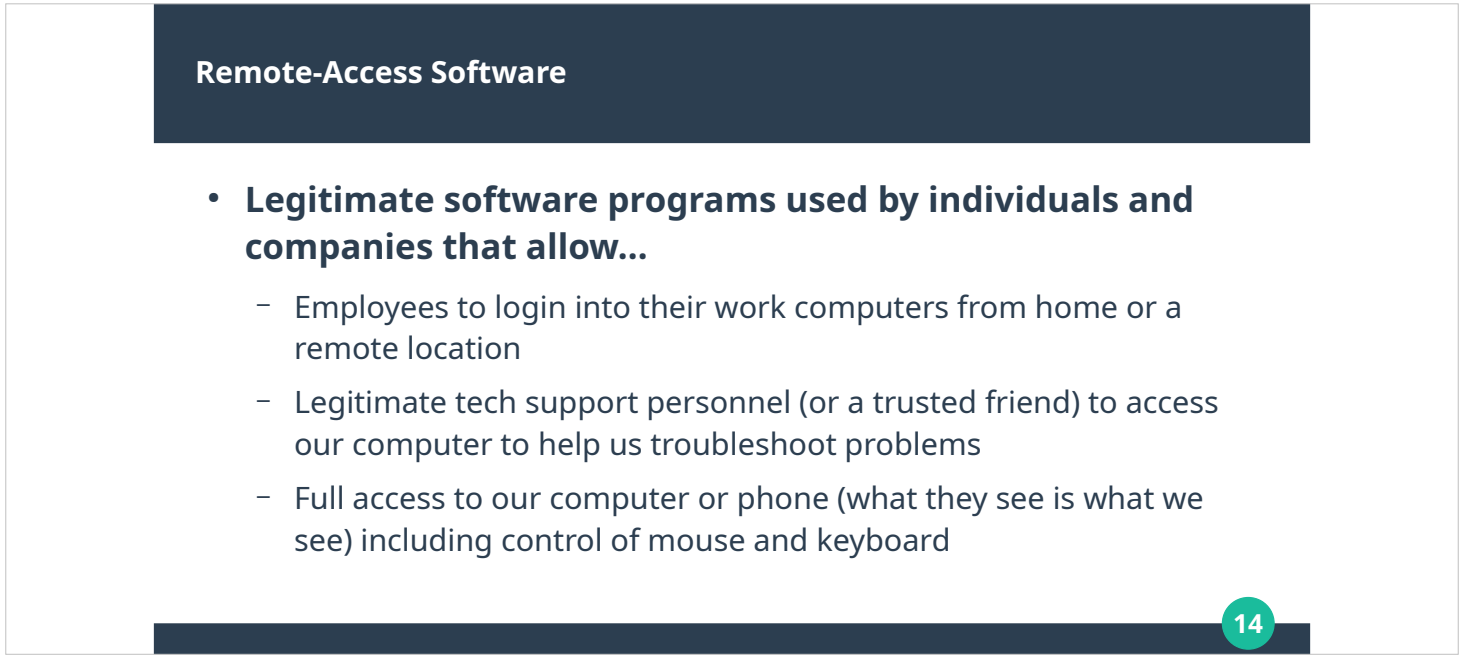
Tech support scams commonly target seniors and those who are not very computer savvy.

Sometimes, scammers spoof or otherwise impersonate government agencies like the FBI or the IRS. This again creates a sense of urgency and we lower our guard, especially if they already have our name, address and other information.

No matter the situation, never download any program, software or app onto your computer or smartphone whether it is an email that’s asking you to do so or a person on the phone. It’s the fastest way for a scammer to gain access to your device and install more surveillance tools or take over your computer.

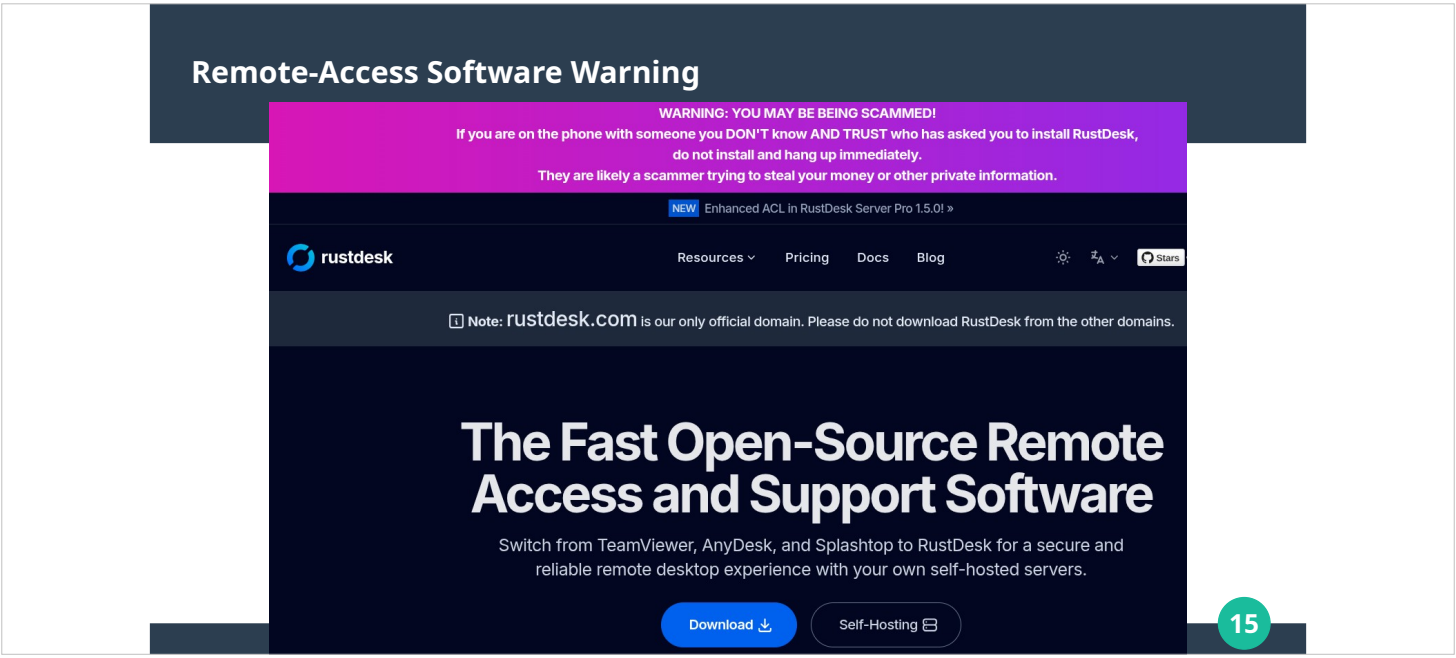
The Federal Communications Commission (FCC) has a webpage on caller ID spoofing. This is the way it works. You get a phone call from your bank. Your phone has the caller ID. It shows the name of your bank which you yourself entered into your phone. There's no reason to believe anything fishy is going on but actually the scammer is spoofing the number. He is calling from his own number but making it appear as if it's coming from the bank's number. Your phone recognizes the incoming number because it is in the contacts and shows the name of the bank on the caller ID. Your phone has no way of knowing who actually is on the other end of the line. There is instant trust because we trust our phones.

Banks rarely call their customers, so be suspicious. Phone numbers, text messages and emails – they can all be spoofed and made to appear as if they are coming from legitimate sources. We should never give out any information when we get a call from the outside even if they claim to be our bank, or the FBI, or the IRS.



I mentioned earlier that scammers sometimes ask us to download and install software. One type of software is called remote-access software. This kind of software has legitimate uses. Employees of a company working from home might use it to log into their work computers and it's as if they are really sitting at their desk at work. They're on their home computer but what they see on it is the screen of the work computer. This is also the software real tech support personnel or a tech-savvy niece or cousin might ask you to install on your computer, so they can see what you see, and help you troubleshoot a problem you're facing.

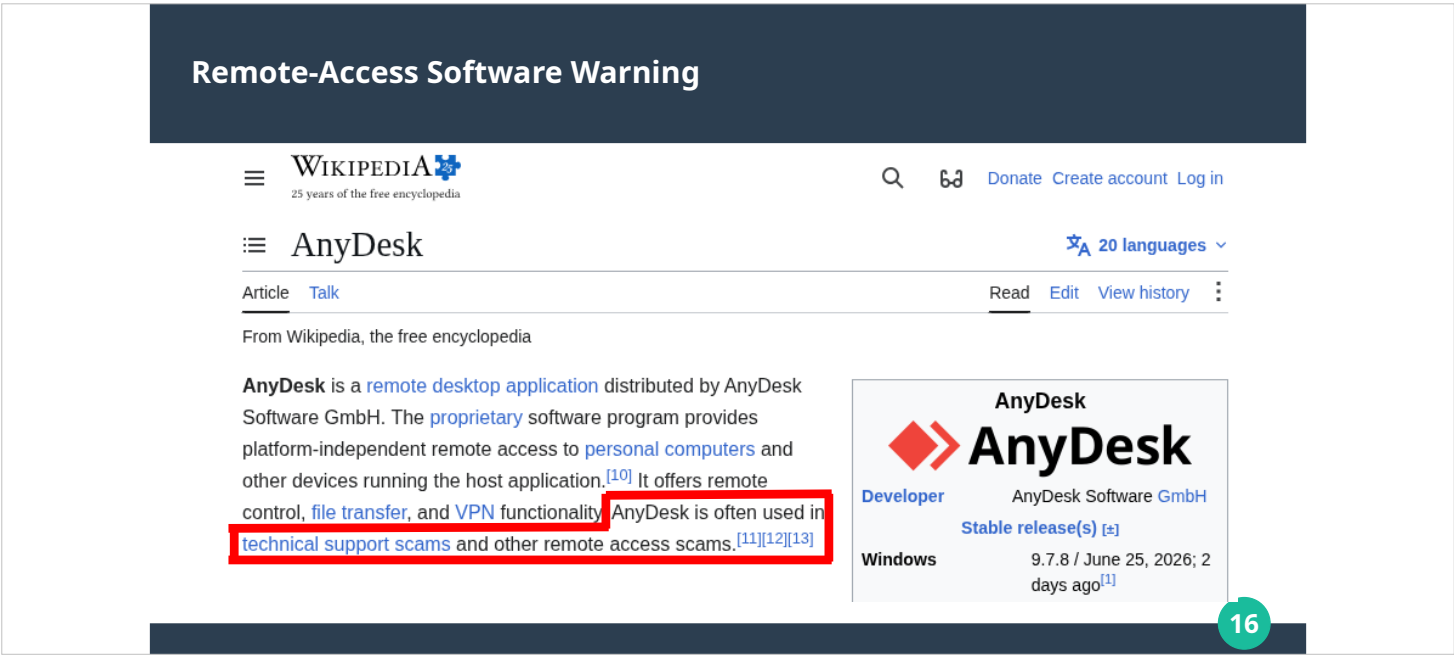
Remote-access software gives the person on the other side complete access to your computer. What they see is what you see. When they move their mouse, you see the cursor moving on your screen. When they type something, you see it appear on your screen. They can download and install anything they want and change any and all settings on your computer. And they could be a thousand miles away. Maybe in Pakistan!



This is the website of RustDesk – a free remote-access software anyone can download and install on their computer. Look at the top of the webpage. There's a huge banner with a big warning on it. It says:

Warning: you may be being scammed. If you're on the phone with someone you don't know and trust, who has asked you to install RustDesk, do not install and hang up immediately. They are likely a scammer trying to steal your money or other private information.

The reason RustDesk, which is a legitimate organization with a legitimate product, has to put up such a warning is because it has come to their attention that scammers are using their product to gain access to the computers of unsuspecting people and they feel responsible enough to warn anyone visiting their website about it. There are many remote-access software products on the market and some of them are free. Not all of them are as responsible as RustDesk.



This is a remote-access software program called AnyDesk and although their website doesn't carry any warning, their wikipedia page says it all:

AnyDesk is often used in technical support scams and other remote access scams.

A scammer can also host RustDesk, AnyDesk or other remote access software on their own website and ask us to download it from there, in which case we won't see any warning. So it's important to remember not to download anything at all when someone asks us to. Hang up immediately.

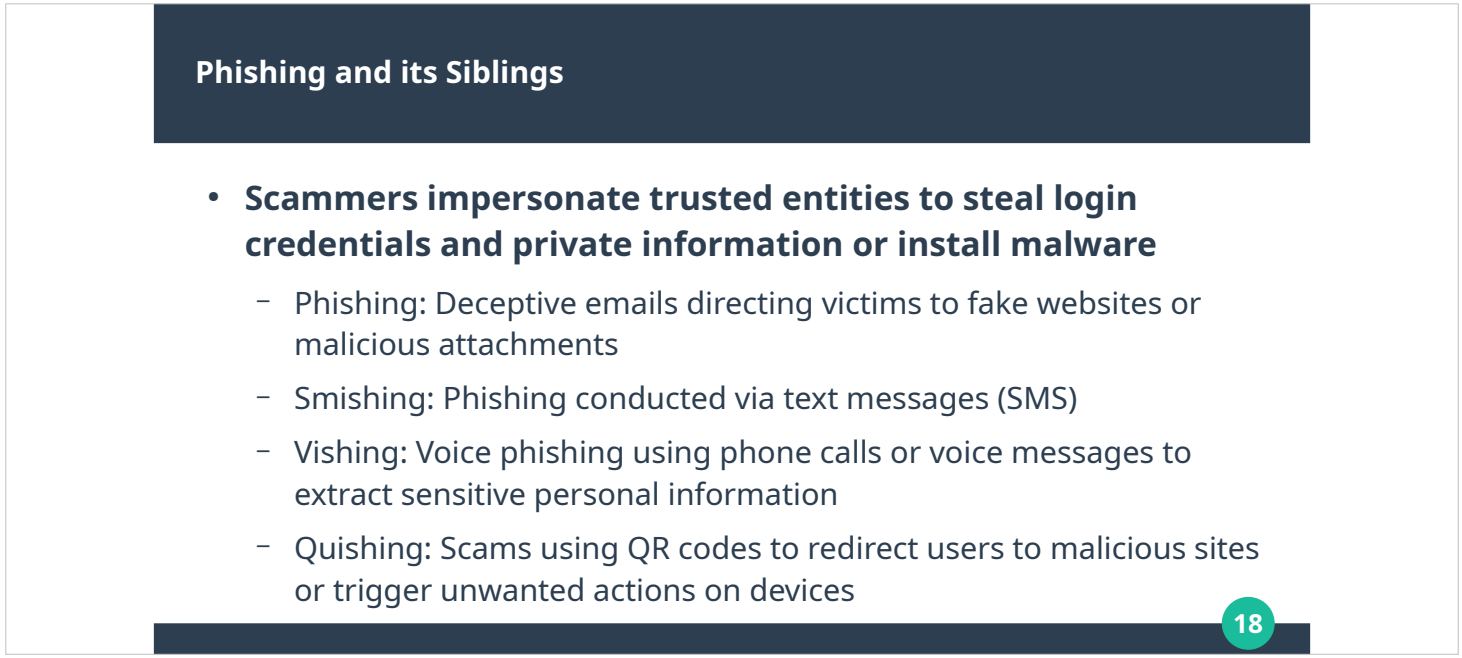
How to avoid tech support scams?

Simply don't engage with any unsolicited contacts, whether it is by phone or text or email. Tech companies like Microsoft or Google don't contact their users to warn them about viruses or to sell them virus removal services.

If you run into a scary-looking screen like the blue screen we saw earlier, be suspicious and don't call the number it says to call, nor click on any links. Simply take a picture of the screen with your phone and restart your computer. The warning will go away. If it appears again, call a tech-savvy friend or a local computer repair shop. Do not search for virus removal software on the Internet. Some of them are malware themselves.

Install anti-virus software. More on this later in this presentation.

Refrain from downloading any software that you're being asked to download and install. Do not even visit any websites that the caller on the other end is asking you to go to. Simply visiting certain websites downloads malware automatically.



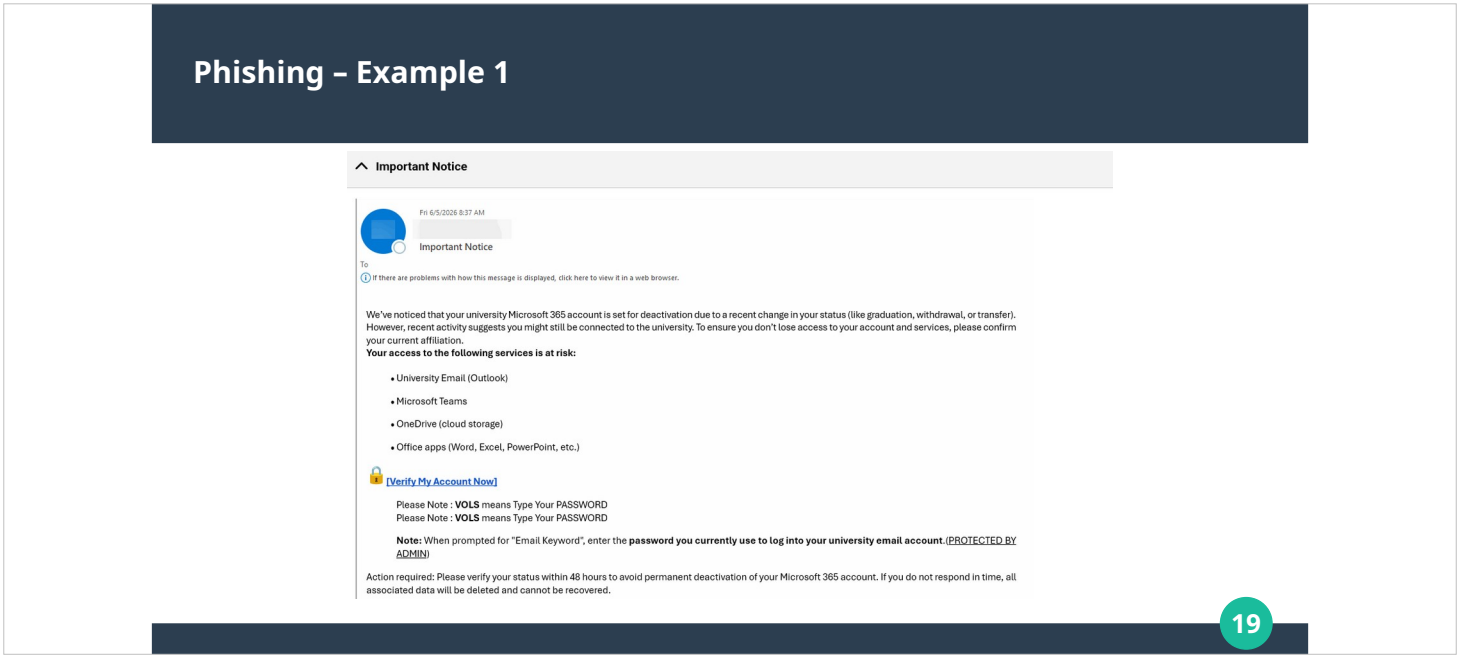
Phishing is a form of impersonation that's designed to trick the victim into believing they are interacting with a legitimate entity, like their bank, a tech company like Amazon, or a government agency like the USPS, and leads the victim into revealing their personal information or login credentials (usernames and passwords) which are then used by the scammer to hack into their accounts to steal money or to sell to other scammers.

Depending on the form of contact, there are 4 variants of phishing. If it's done by email (an email appearing to come from a legitimate source), it's phishing.

If it's done by text message, it's called smishing (s is for SMS or text).

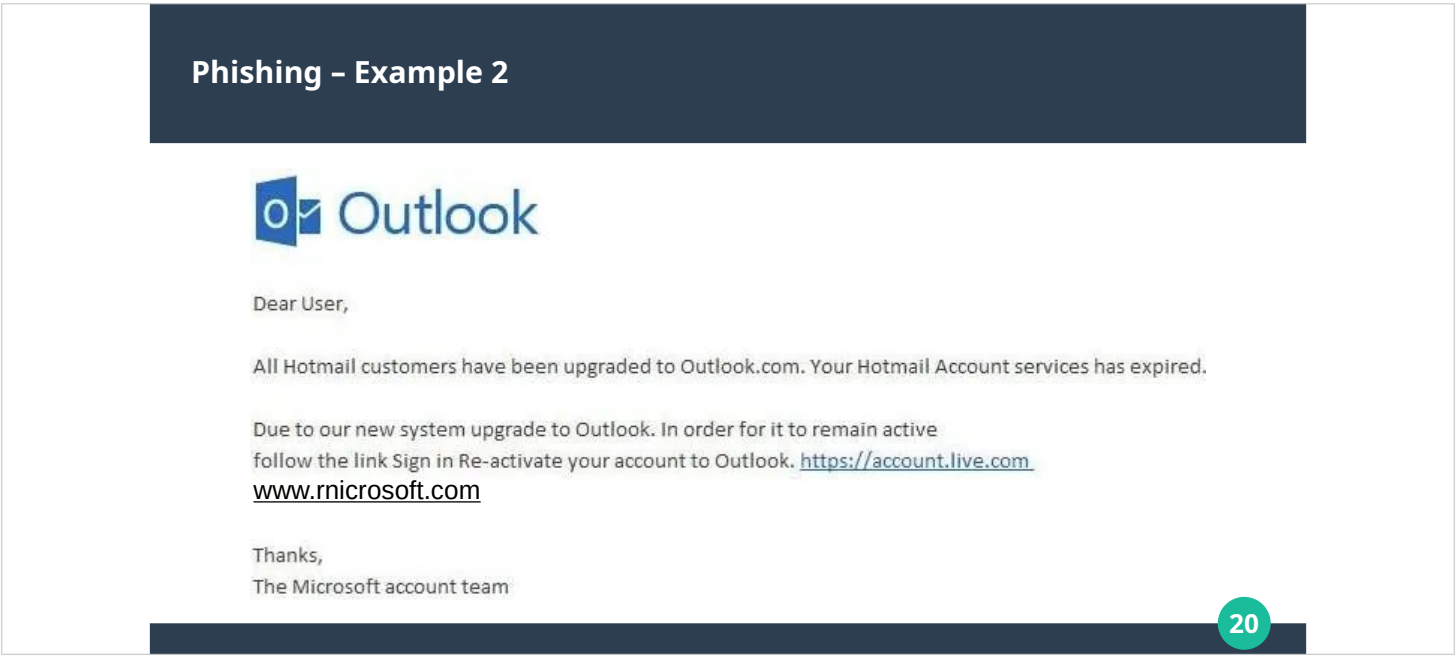
If it's attempted over a phone call, it's called vishing (v for voice).

And over the last several years, a new sibling has joined in – quishing, which is when QR codes are used to redirect victims to fake websites, or trigger unwanted and dangerous actions on their devices. We cover QR codes in a few slides.



Here's an example of a phishing email. It is targeted at a student and it appears to come from their university. It says that because they have graduated, they might lose access to their account unless they click on the link below and do something. It sounds reasonable. A scammer can easily target a thousand new graduates of a university with such an email and expect a decent number of clicks on the link from unsuspecting students. The link leads to a fake website that is designed to look like the real university student portal where the victim enters their login and password, which the scammer immediately collects.

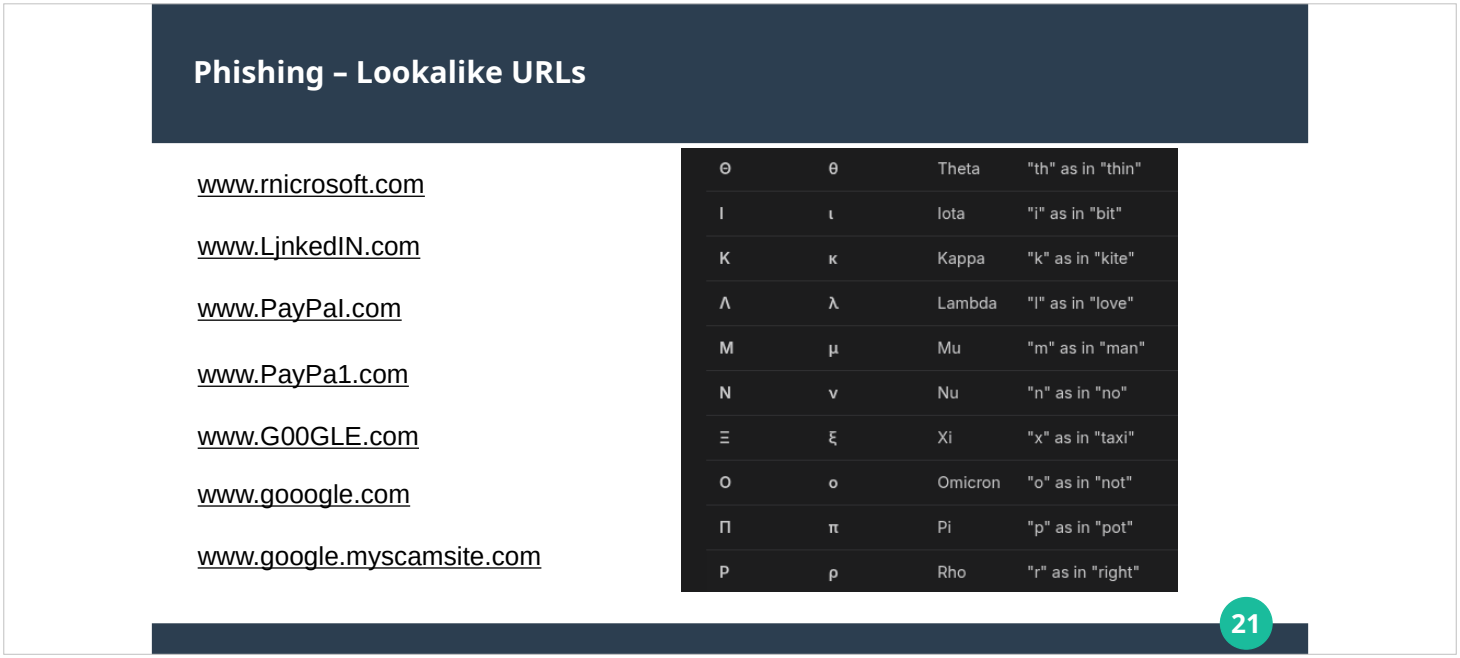
At the bottom of the email, there is a warning saying the account will be deleted unless the student acts within 48 hours. This creates a sense of urgency and immediacy that discourages the student from putting it off or from doing due diligence. Creating a sense of urgency is a common aspect of phishing emails. A legitimate communication would give much more time, measured in weeks or months.



Here's another example of a phishing email that appears to come from Microsoft's Outlook email service. Again, it looks legitimate at first glance with the Outlook logo and the signing off by "The Microsoft Account Team". But notice they have a bunch of grammatical errors. Grammar errors are the first sign of a scam email because many of these emails are written by foreign scammers whose native language is not English. They can copy the logo from the real website and stick it in an email but they make mistakes drafting the language in the email.

An email can carry a link that on its face says account.live.com, but on the backend, point to a completely different website, possibly one that was created by the scammer. If you hover your mouse on the link, you can see what it's pointing to but if you're looking at the email on your phone, there is no such facility, so it's best not to click on any links in suspicious emails.

Notice the other link. It says "microsoft.com" Or does it?

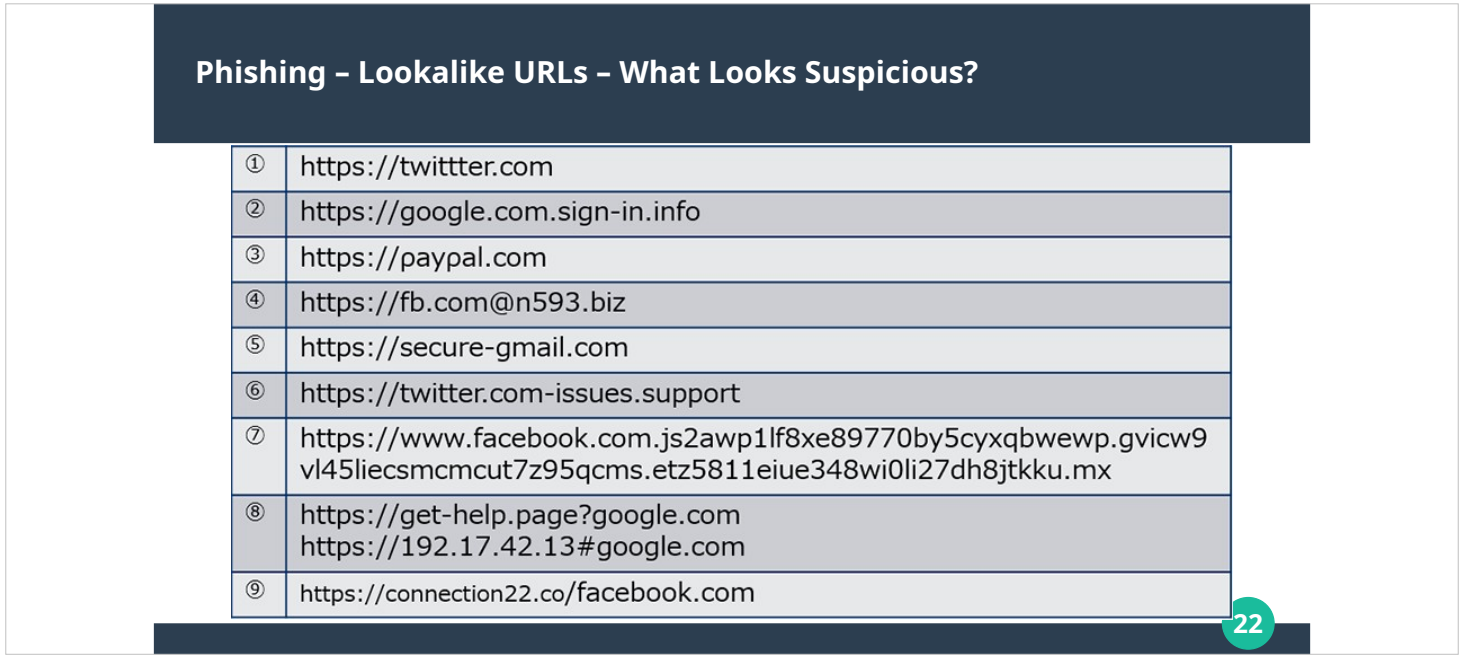


Can you read this first URL here? It's a lookalike URL – made to look like microsoft.com but it's actually not an 'm' but an 'r' followed by an 'n'. Scammers come up with such URLs in an attempt to trick our eyes into believing it's a legitimate URL of a well-known company.

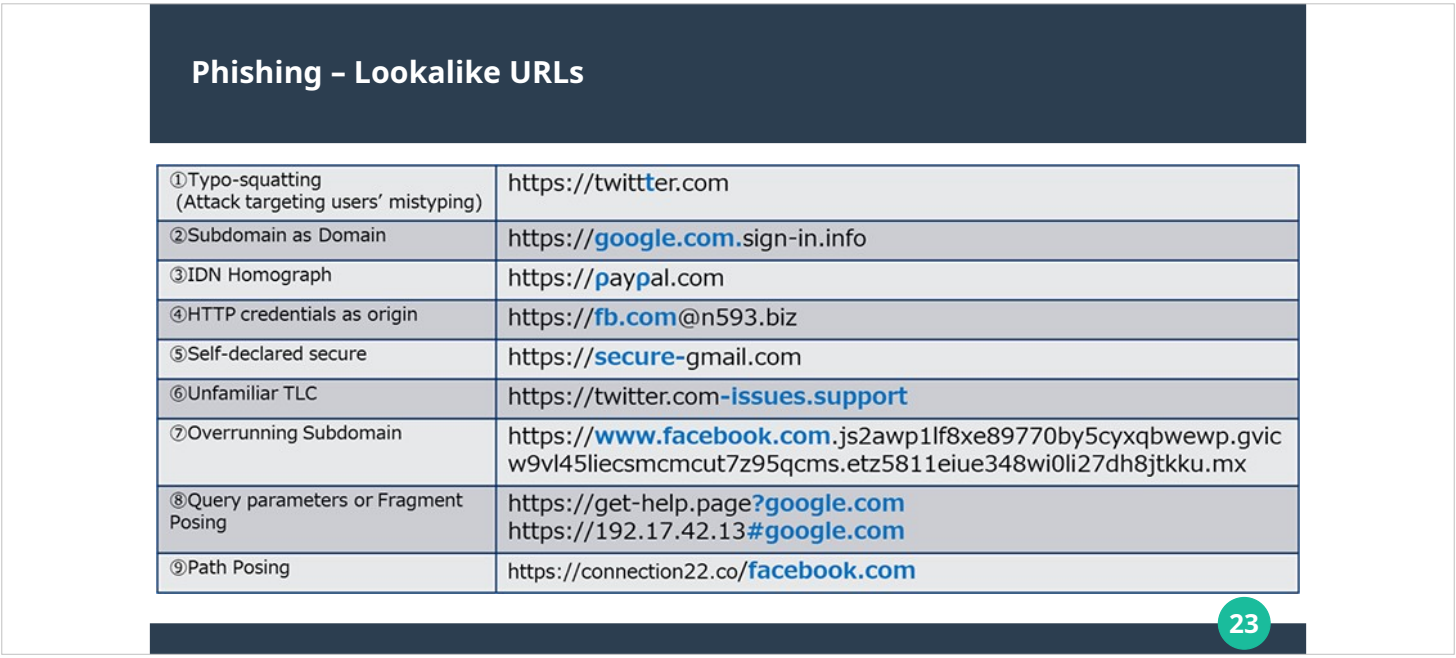
They substitute one letter with another letter or number or a greek character that looks similar. Once they acquire this lookalike URL (also called a domain name), they create a fake website that mirrors the real one and it's ready to collect unsuspecting victims' personal information.

Look at the URLs in the list to the left and see if you can spot the spurious characters.

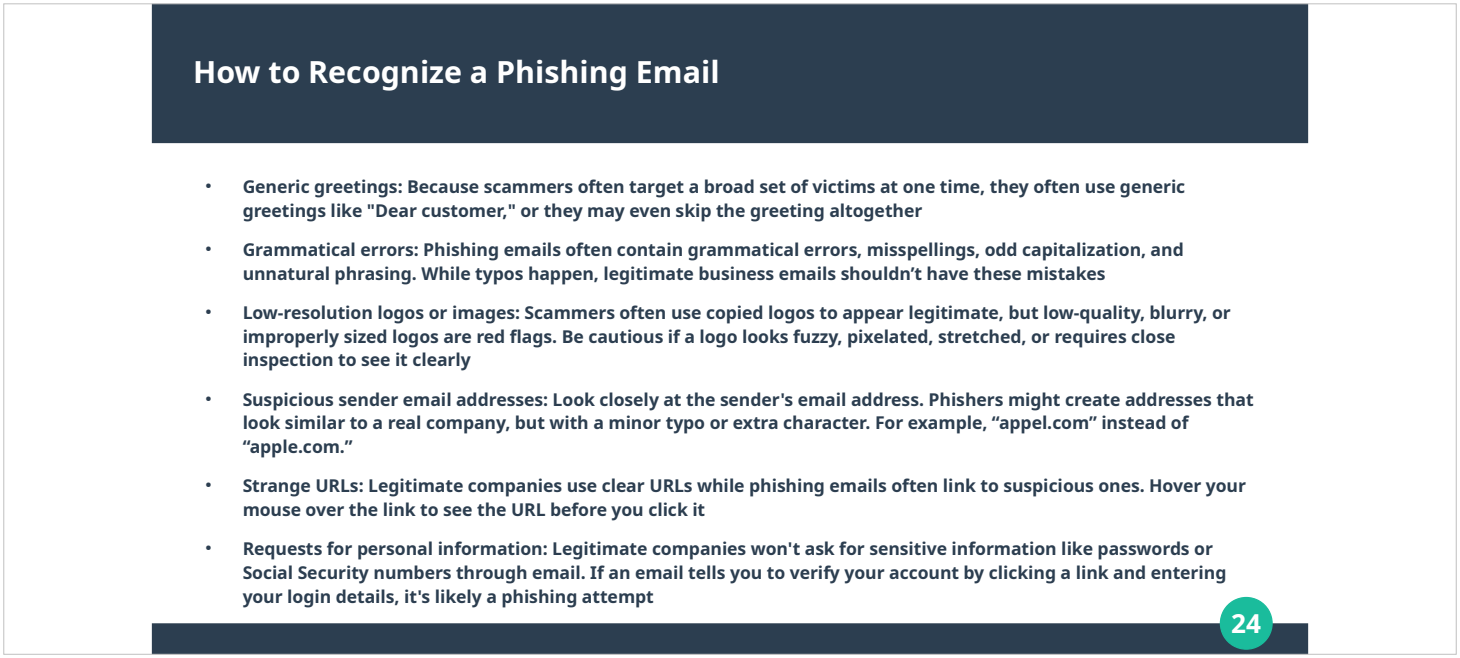
On the right is a table of Greek letters, some of which appear very similar to certain letters in English. For example, the Greek letter Rho looks a lot like the English letter p.



Take a look at the URLs here and try to assess if they are real or fake! The key to this puzzle is in the next slide!



1. There's an extra t in twitter's lookalike URL
2. The actual site is sign-in.info. They simply created a sub-domain called google but it has nothing to do with Google.
3. The Greek letter Rho is used instead of a p, but it looks like paypal.com
4. The fake website is n593.biz, nothing to do with facebook.
5. The fake website is secure-google.com, not associated with google.com
6. com-issues.support has nothing to do with twitter
7. facebook is a sub-domain – a part of a larger scam site. Not associated with facebook.
8. google.com is added at the end of the URL and is not the actual URL, hence not associated with Google.
9. facebook.com is simply a path on the web server, the website being connection22.co, which is a fake website created by scammers.



There are certain clues that might help us determine if an email or text message is a phishing scam.

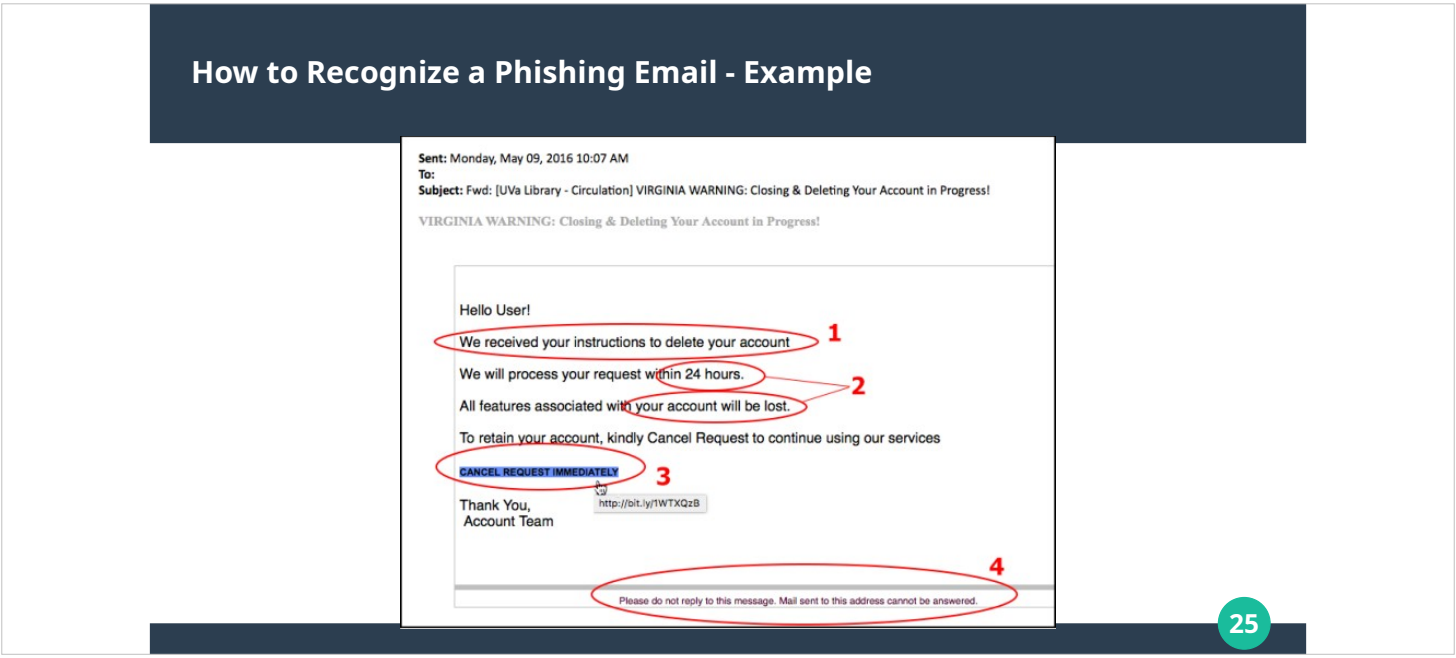
They tend to use generic greetings like Hello User instead of your name. However, know that it's quite easy to greet you by your name too, because if they have your name (and your name is out there along with your email address), it's trivial to include it in a phishing message with just a little skill.

We talked about grammatical errors, generally coming from foreign scammers but again, be aware that they're using AI more and more and the English is flawless.

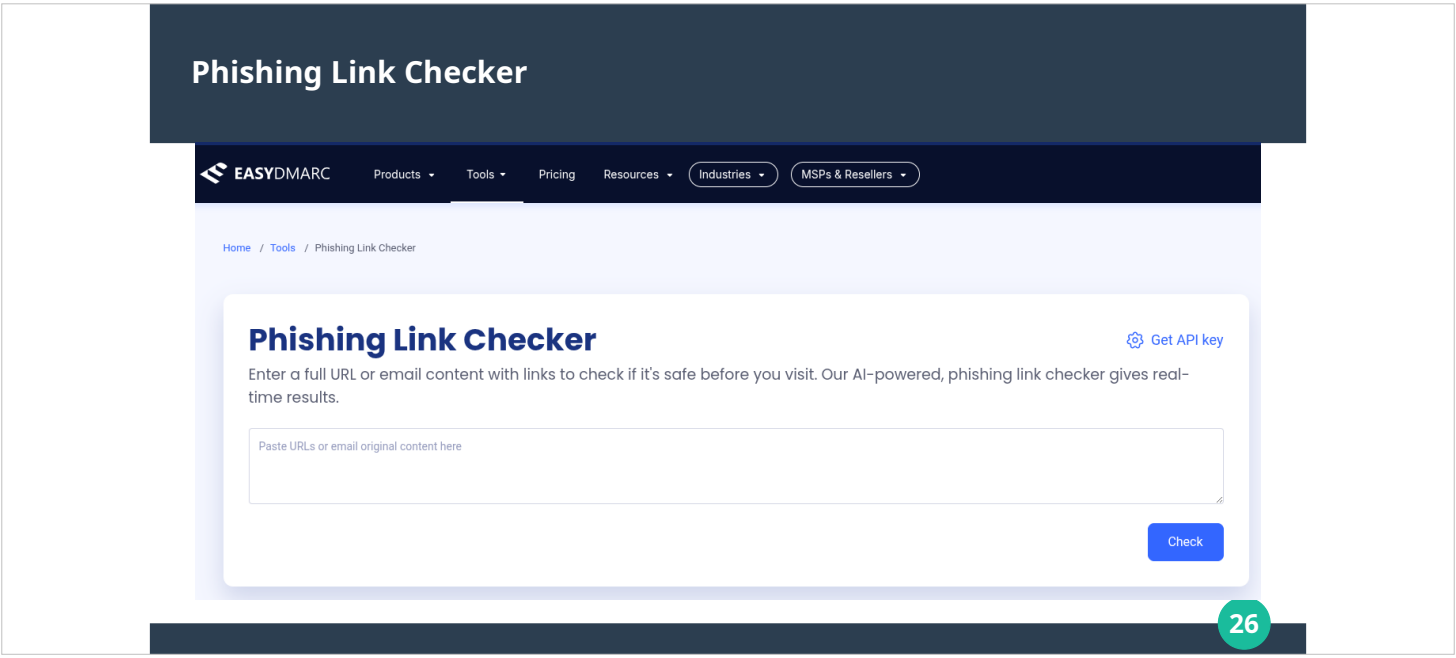
Images and logos that are blurry or out of proportion, because these are copied from the real websites and may not transfer properly to the phishing message.

Presence of lookalike URLS like the ones we just saw. Look at the sender email address while being aware that it can be spoofed. If it looks right, it doesn't mean it's not a phishing message but if it looks suspicious, that's certainly noteworthy.

An urgent tone or a request to verify something or an outright request for personal information

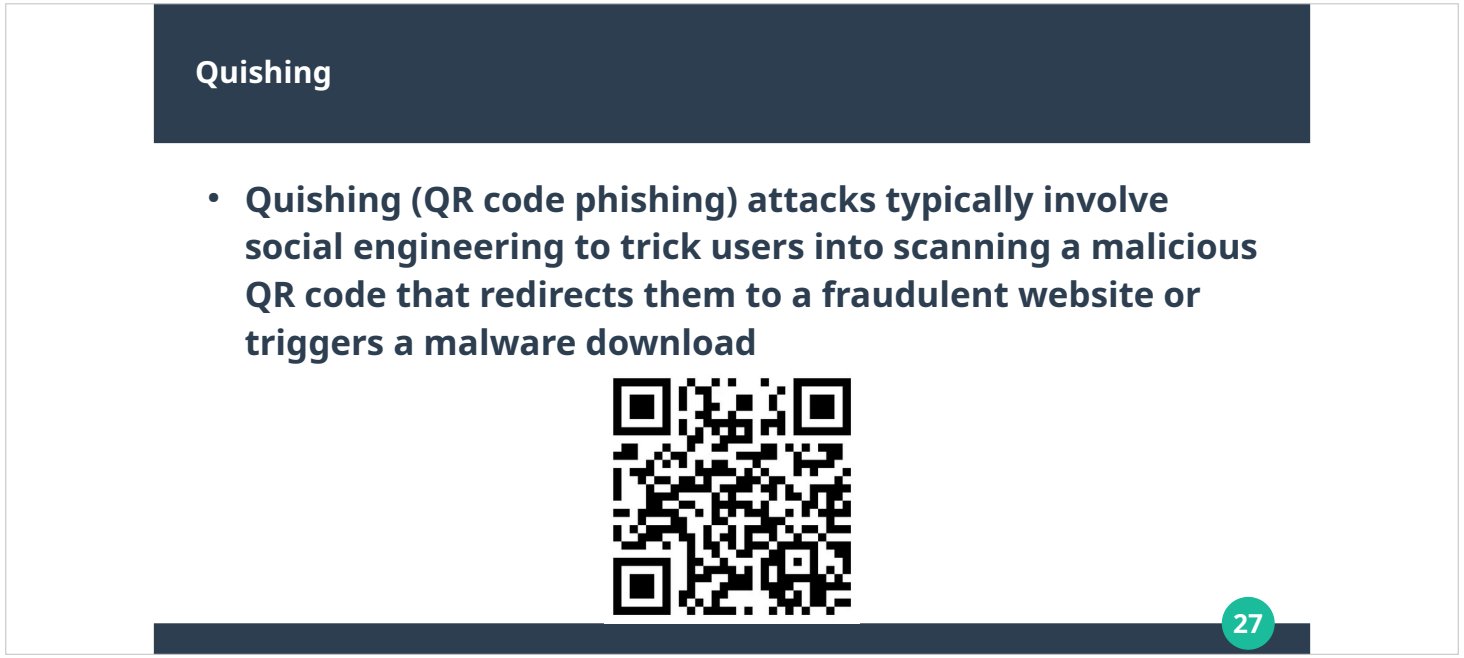


An example.
Some of the things we look for in an email -
Generic greeting – “Hello User” instead of your name.
All features associated with your account will be lost – a sense of urgency requiring you to act immediately, which in this case, to click on the link.
Suspicious URL when you hover the mouse over the link.
These are some tell-tale signs that this might be a phishing email.
There are several examples of phishing emails on the Internet that describe what to look for, so you can develop the sense of discernment that will soon become an effortless habit.



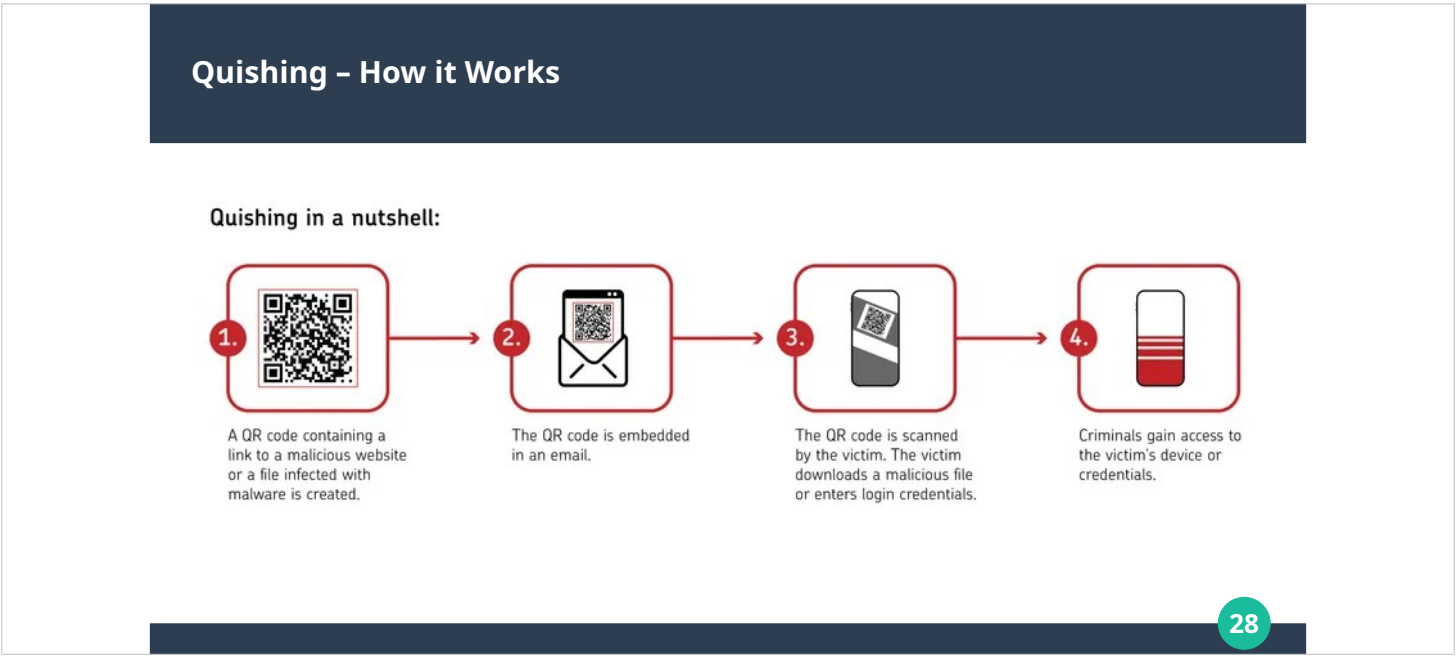
If you get a message or email that looks suspicious but you can't quite tell, there's a tool on the Internet that you can simply paste the entire text of the email into, and it will tell you if there is anything fishy going on.

It will scan the URLs in the email body and show "suspicious" if it's not a legitimate email.



In recent years, QR codes (short for Quick Response), like the one shown here have become commonplace. They're like barcodes but pack more information into the square and are completely unreadable by humans. This makes it hard to ascertain what URL it is actually pointing to. They can be convenient if you know the source, like when you are in a restaurant and there's a QR code as an option to pay the bill. It's easy to scan it with your smartphone and it brings up the payment website or app, so you can make a quick payment. No need to type in a web address into the browser. So, by all means, scan a QR code if you trust the source and the placement.

On the other hand, if you see a QR code on the street or on a storefront facing the street, be aware that anyone could have posted it there. Scanning such a QR code with your phone could take you directly to a malicious website.



QR codes can be embedded in an email or sent via text message. They can be displayed on flyers and advertisements. They can be posted on restaurant windows asking for reviews. They're often used for electronic tickets to events and on airline boarding passes. Since they're more convenient than paper tickets and all it takes to scan one is a smartphone with a camera, which everyone has these days, it's easy to get used to them and let our guard down.

When we enter what I call the "cybersafe mindset", we become aware of the circumstances, the time and place we're at, and the source of the QR code. Before we scan one, we stay alert to the possibility that it might take us directly to a malicious webpage where a malware file is asked to be downloaded to our device.

It's an unfortunate trade-off in the world of technology that more convenience generally means a higher risk of exposure to security threats. However, with a little practice and care, we can have the convenience while still being alert to the risks.

Quishing – Parking Meter Scam

29

One of the places the QR code makes its appearance is on parking meters. Compared to installing a cash and coin payment machine, it costs less for the parking company or the local government to direct customers to an online portal where payments can be made with a credit card. It's also more convenient for the customer but therein lies the risk.

This is a true story. It has happened many times in many places.

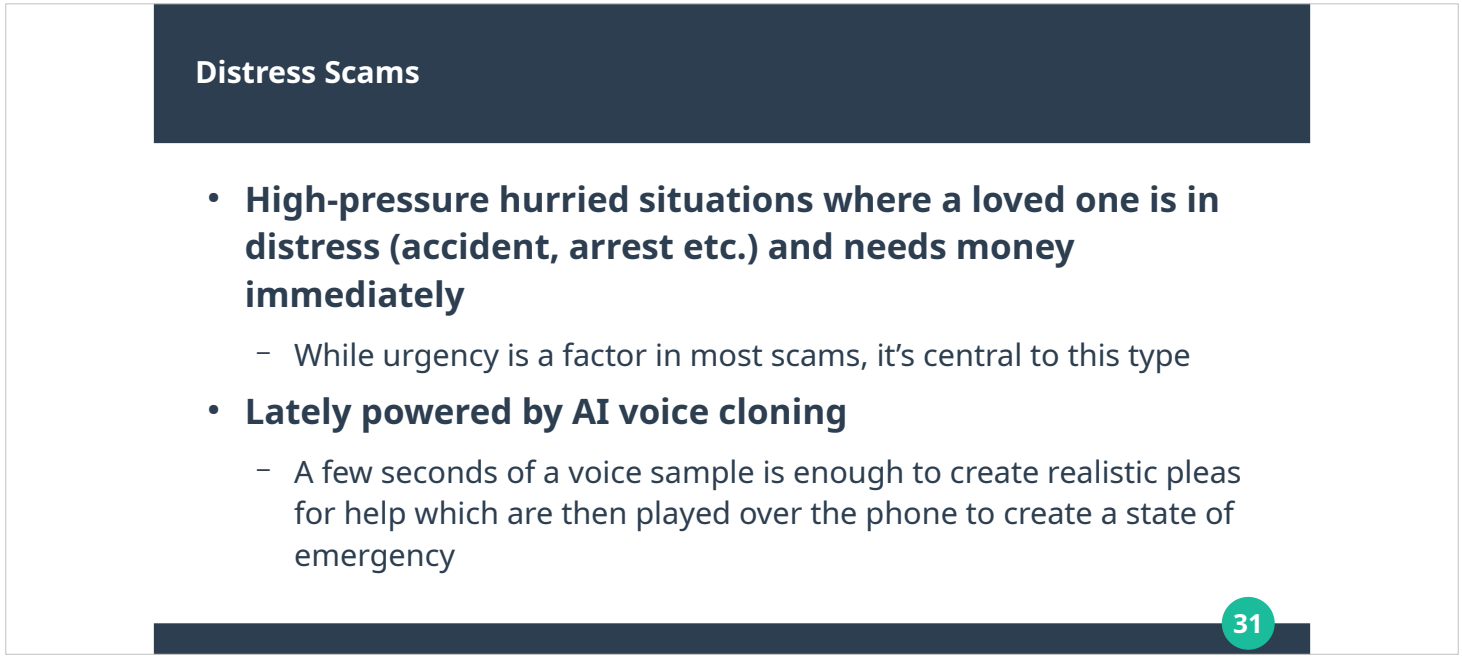
Quishing – Parking Meter Scam

30

The customer scans the QR code and is taken to a payment website that looks authentic. The payment is made but upon return to the car, a parking ticket is found on the windshield. The company never received the payment because the customer ended up being scammed. A scammer stuck a different QR code pointing to a fake website on top of the original QR code. It’s extremely hard to tell that a fake QR code is stuck on top of the real one unless one looks closely.

Now, the scammer not only has the customer’s money but also the credit card details.

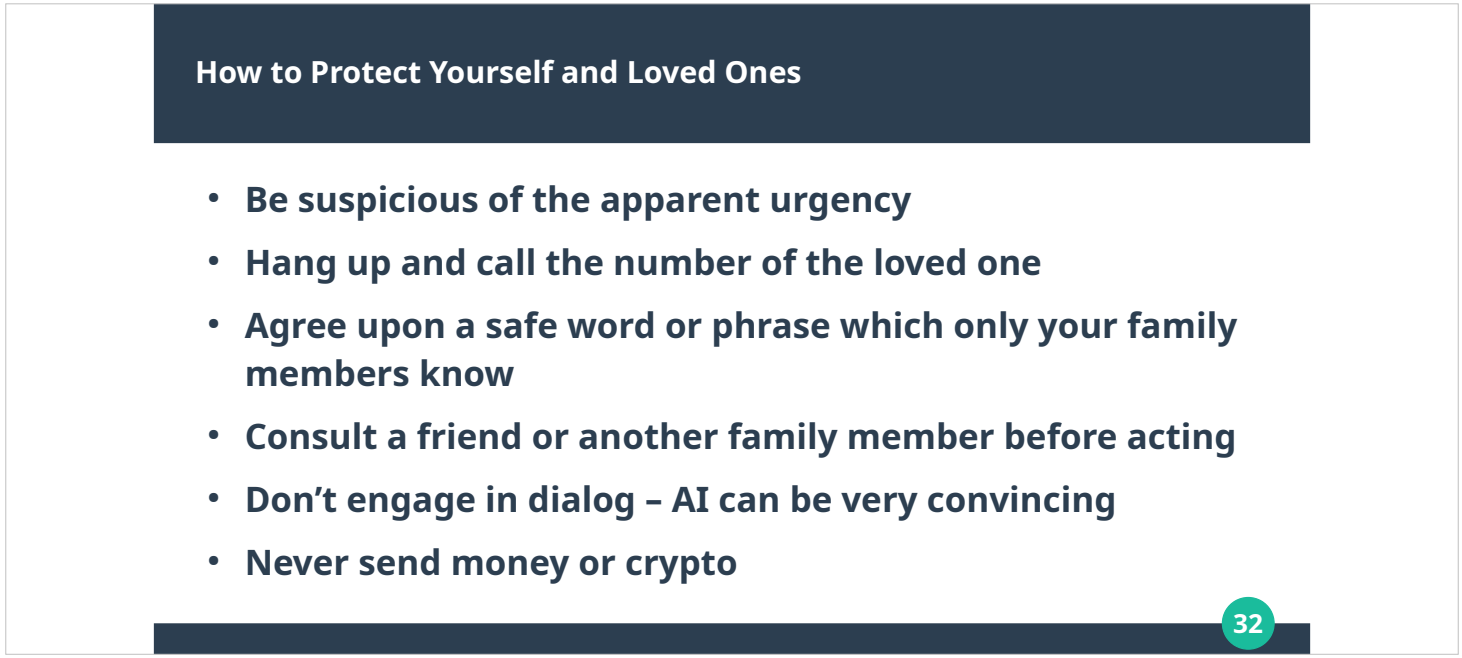
It’s best not to scan any QR code that might have been tampered with. That’s essentially any QR code in a public place, or on a flyer in your mailbox.



Distress scams are on the rise. They catch us by surprise and spur us into rescue mode because we're told that someone in our family, a niece or a grandson, is in an emergency. The emergency could be anything, an auto accident that required a niece to be rushed to the ER and now requires immediate surgery, or a grandson who was arrested and needs bail money right away.

To make it all convincing, it is your niece or grandson on the phone asking for help. Or is it? With the help of AI, scammers have been getting good at cloning the voice of everyday people to enable these scams.

Research has shown that as few as 10 seconds of someone's voice is enough to feed to an AI model, and then prompt it to create any arbitrary speech in that voice. I have seen recommendations to remove our voicemail greetings where we say our name and leave a short message for the caller. Those few seconds of our voice are apparently enough to fool our friends and relatives into believing it's us in distress.



How to protect yourself and loved ones from distress scams:

If the matter is urgent, it’s a reason to be suspicious. Urgency is a feature of most scams but is the defining feature of a distress scam.

Hang up and call the loved one yourself from your own phone, and if you can’t reach them, ask around and investigate. Share the “news” with family and check if it could be true.

Agree upon a safe word that only you and your family members know. If you get a distress call, ask for the safe word. An AI on the other end wouldn’t know the answer.

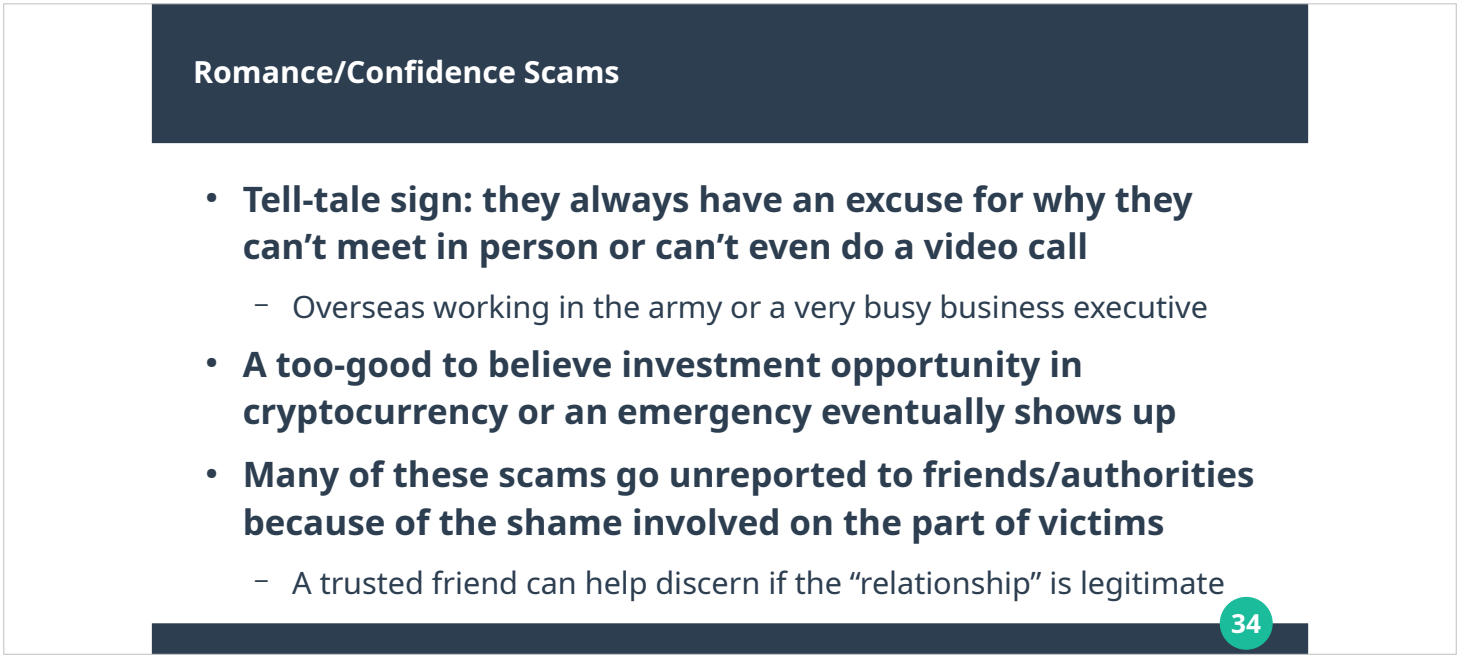
Do not continue engaging with the caller. Resist the temptation to test the AI yourself even if you suspect it, because AI models these days can very convincingly hold a conversation like any other human being.

Never send any money, especially crypto currency. If you’re asked to deposit cash into a Bitcoin ATM at the local convenience store, be very suspicious.

Romance scams have increased in number in the age of social media. It's easy to create a fake profile, upload a fake photo, and pose as the perfect partner. Scammers exploit loneliness and slowly build trust over time, typically weeks and months, before making a request for money. Meanwhile, they collect lots of information in casual conversation. This information can be leveraged for future scams, or sold to other scammers on the dark web.

Even though it takes more time, the scammer gets a larger payout from this type of scam, because the victim trusts the scammer and suppresses any doubts that arise in their mind as to whether they are being taken for a ride. Victims also tend to discount any warnings that friends and family give them.

Scammers are even learning to use AI to carry on conversations on their behalf. They may step in from time to time and keep the dialog going, while they manage multiple "clients" at the same time. There is a video on this topic in the Resources section of the website lakelandcybersafe.org

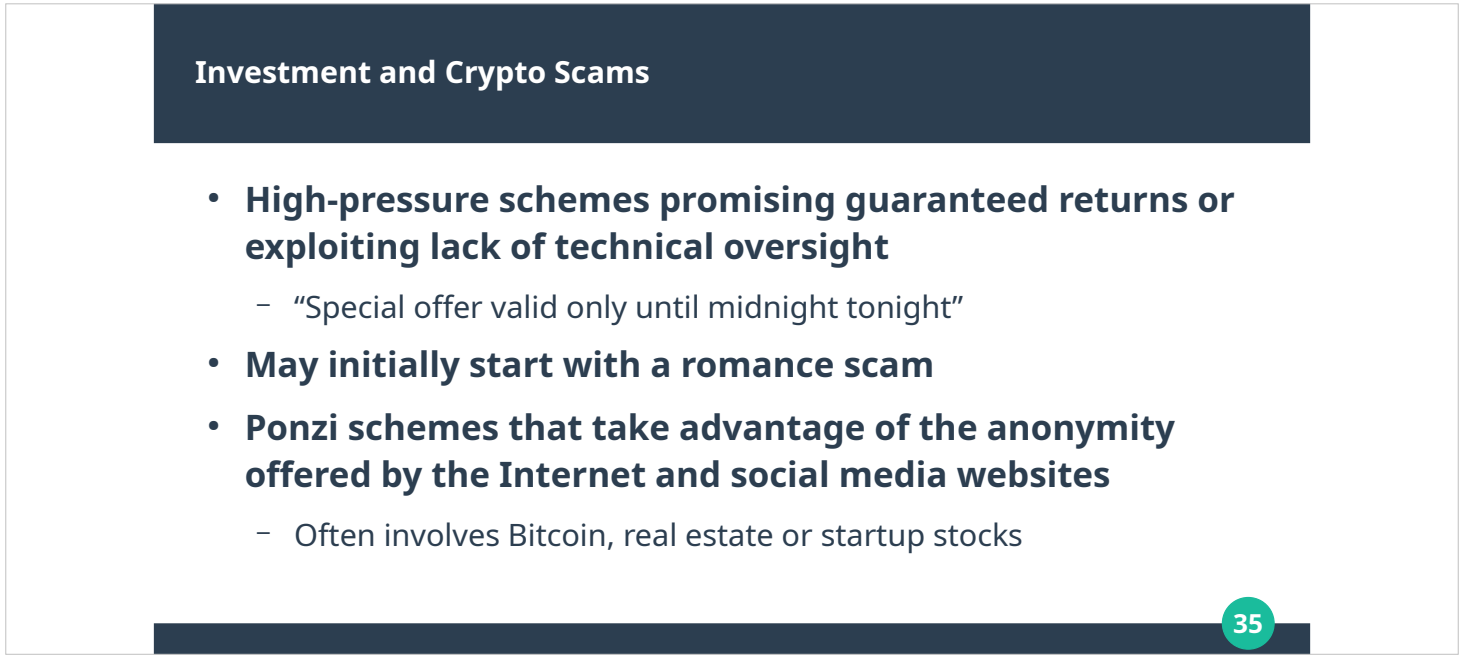


One tell-tale sign of a romance scam: the scammer always seems to have an excuse why an in-person meeting can't happen just yet. They may claim to be overseas serving in the military, or just busy with their business.

After some time spent building a romantic long-distance relationship, inevitably, an emergency or another reason pops up, requiring immediate funds, and "would you help them out"? Or it is a really good company they have been working to build, and you're invited to invest for quick high returns.

Thus a romance scam morphs into a cryptocurrency scam. Note that, ultimately, the scammer is after money, while the nature of the scam itself varies and changes.

A romance scam victim suffers from immense shame and avoids reporting to authorities, or even sharing with friends and family. Shame suffered by scam victims and the concealment of the scams often leads to under-reporting of actual losses during investigations by authorities. It is an understandable human trait.



Investment and cryptocurrency scams.

The ability to email and text people en-mass has made the age-old investment scams cheaper and more effective to carry out.

It takes pennies to send out a slick marketing email advertising a new investment opportunity. It could be real estate, a bitcoin startup, or a new way to invest in high growth stocks.

Investment scams may stand on their own or start off by building trust via a romance scam.

They typically start on social media, or arrive in your email inbox, and might point to a slick marketing website that displays a countdown to the end of the current round of investment, creating that sense of urgency.

Fake 5-star reviews and endorsements by celebrities are sometimes part of the "fundraising" operation.

Anonymity on the Internet

An Internet meme from 1993

"On the Internet, nobody knows you're a dog"

36

This is a meme from 1993, a time before the Internet became popular. The caption reads, "On the internet, nobody knows you're a dog".

It captures the essential principle of anonymity that the electronic medium of Internet offers, something the scammer takes advantage of while looking for any and all information about us.

Scammers use various techniques to hide their true identity and location. They use burner phones and virtual phone numbers that are difficult to trace while insisting that they are located in an American city. There are numerous videos of real scam calls on YouTube and I recommend watching a few of them to get an idea of how they work.

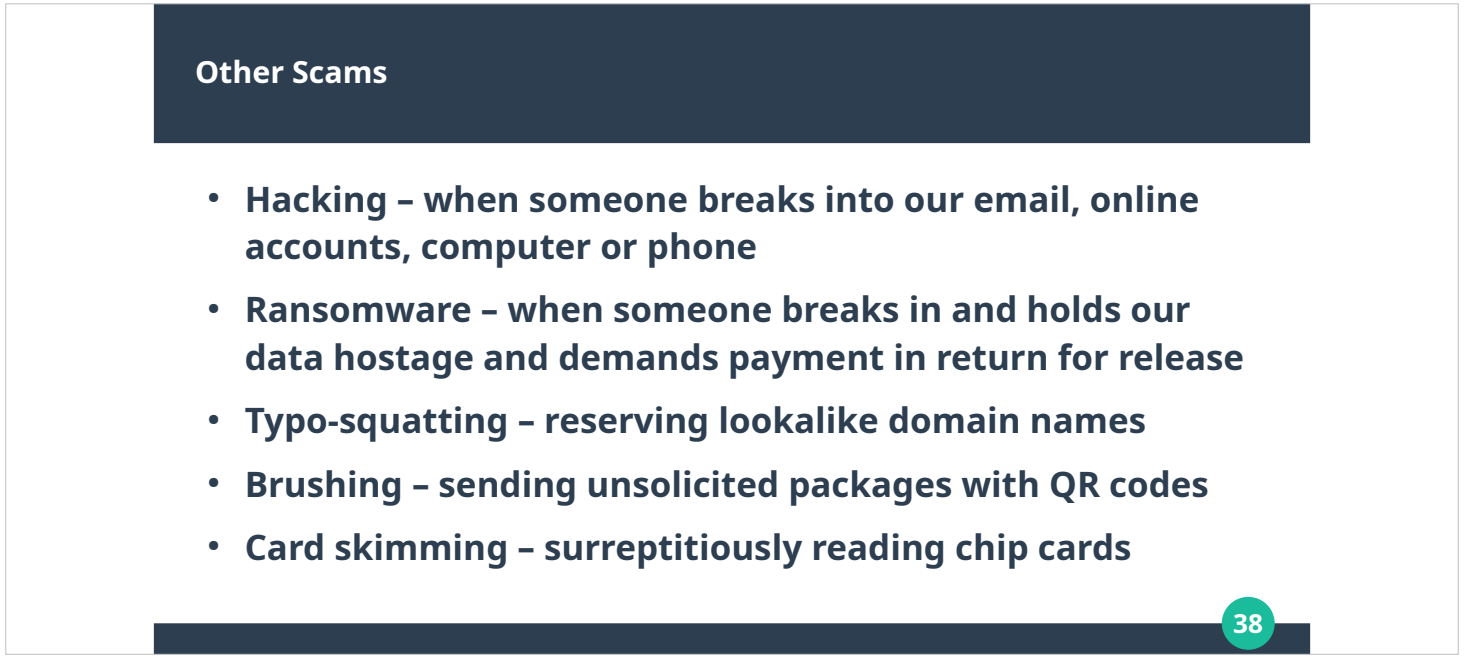
Anonymity on the Internet

Now, the dog has learned to use AI

Bottom-line: Careful who you trust on the Internet!

37

A more recent version of the meme has the same caption but a different dog. This dog has learned to use AI!
I don’t have anything against dogs. I like dogs. But scammers, not so much!



Some other types of scams I will quickly go over.

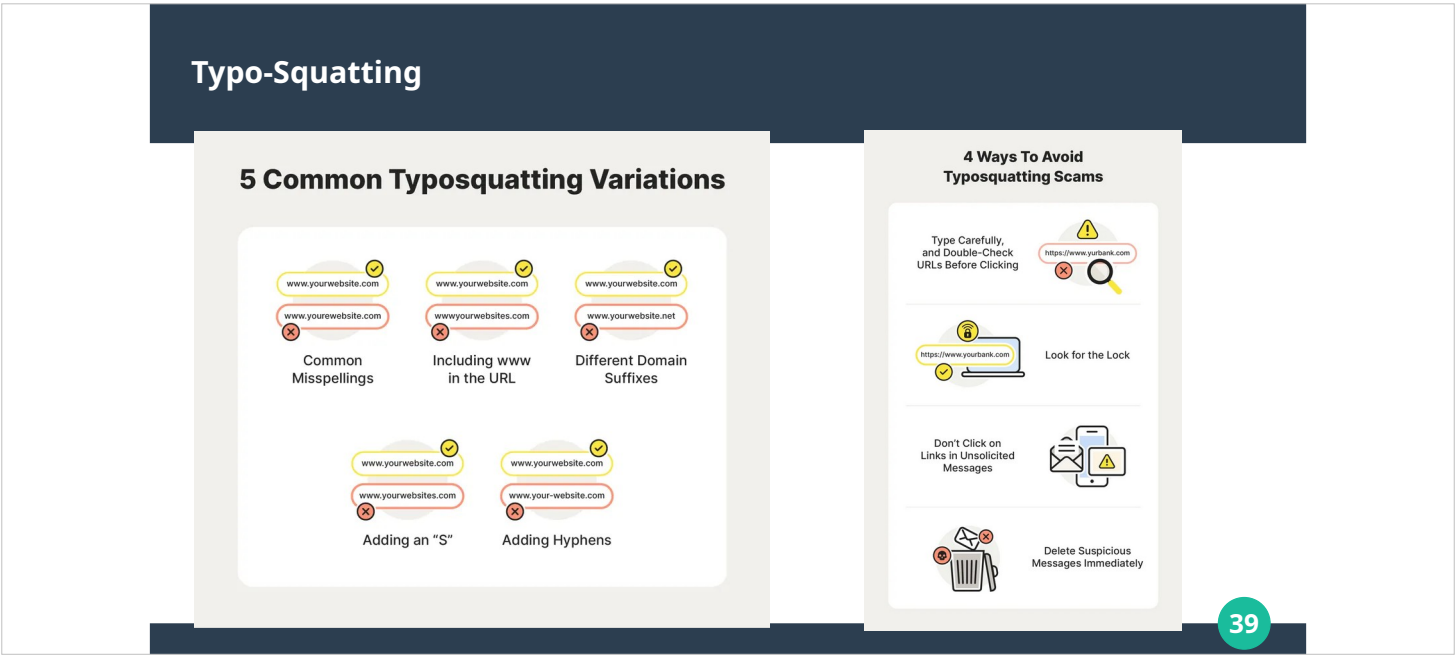
Hacking – this is when someone specifically targets a victim, as opposed to casting a wide net and waiting for victims to bite. A hacker picks a target and goes after them to defraud them by breaking into their devices or online accounts, generally keeping the victim completely in the dark.

Ransomware – this affects companies and governments more than individuals, but can happen to anyone. A hacker locks up all the data and systems that the company relies on for daily operation, rendering them unusable, and demands a ransom to unlock them.

Typo-squatting – we get into this in the next slide.

Brushing – when we get an empty package in the mail that has nothing but a QR code in it and we scan it out of curiosity and get taken to a scam website.

Card-skimming – when a scanner is used to read the information in our credit cards.



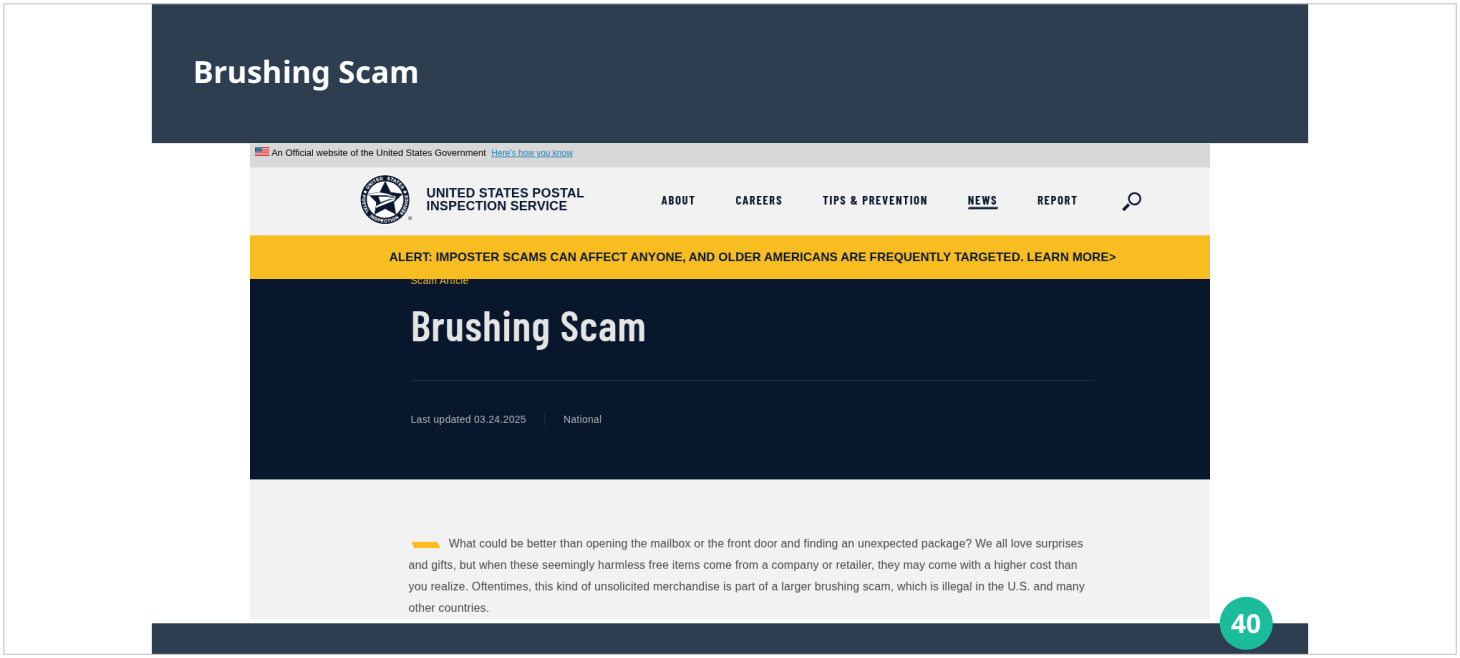
Typo-squatting is a little different from lookalike URLs, which we discussed earlier.

A lookalike URL is what we get in an email or text and we click on it and it leads us to a scam website.

But sometimes we might make a mistake while typing in a URL into the browser and end up on a fake website that looks like the real one. In this case, a scammer has intentionally created the website with a typo in it, knowing enough number of people will make the typo and end up on their site.

Sometimes, a legitimate website ends in .org or .net but a scammer might acquire the same website ending in .com, knowing enough people will type in .com trying to reach that website.

Big companies typically register multiple domain names that are adjacent to their actual domain names to prevent typo-squatters from getting their customers' traffic but we have to be on our own guard and double-check what we type in.



Brushing scams are a relatively new trend. Here's an article on it from the US Postal Inspection Service.

They take advantage of the basic sense of curiosity that's part of human nature.

Mysterious packages are sent out to hundreds or thousands of people. The scammer already has our names and addresses. We certainly didn't order anything recently, so we open it with curiosity, but there's nothing in it but a paper slip with a QR code on it. If we scan it, we are immediately taken to the scammer's website, which might be a source of malware or might present a phishing attack. The scammer can also customize the QR code in such a way that they know exactly who among the people they sent the packages to is now scanning it and visiting their site. In addition to our name and address, they now have our IP address, browser and other information.

Also, when the USPS delivers a package, the sender also comes to know that the address is current and valid. This verified address fetches a higher price when sold on the dark web to other scammers.

You may have seen this in the local news or in a crime investigation report.

Scammers install their own card reader on top of the original card reader in a gas station, on an ATM, or inside a convenience store. The more sophisticated ones are hard to detect and send all the details of the cards being scanned to the scammer via a radio link in real-time.

This type of fraud has been around and isn't related to computers and the Internet, but I include it in this cybersafety presentation, because it's a good example of the necessity of being aware of how we use our conveniences. Cards are more convenient than cash but they also present certain risks that we need to be aware of. There's a video on this topic on the Resources page of the website lakelandcybersafe.org

The newer cards with chips in them instead of magnetic strips are also susceptible to scanners stealing information off of them. These cards use a technology called RFID (short for Radio Frequency ID), which sends out information stored on them when activated by a radio signal. When you tap a chip card at the grocery checkout, that's what's happening. A small radio frequency activates the chip and a payment is made.

Unfortunately, a scammer can bring a portable scanner close enough to a chip card and swipe the information off of it.

Proximity cards like the ones employees use to enter their office buildings work on the same principle of RFID, and can be scanned and duplicated.

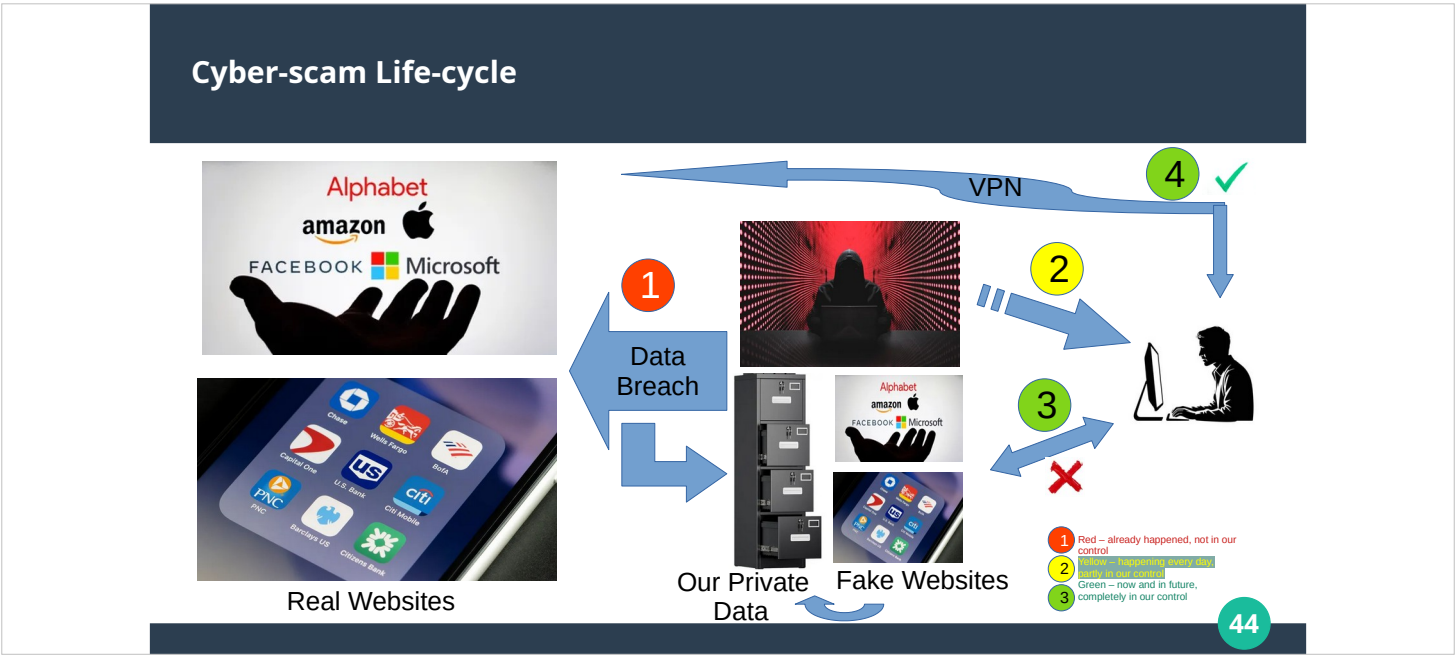
Card Skimming Prevention

43

To prevent such theft, you can place your chip cards in a sleeve like the one shown here. There are also RFID wallets that block RFID scanners from activating the cards stored in them.

We saw so many different types of scams. Is there a way to make sense of them all? Are there certain common elements or patterns among them? Or do we need to remember the intricacies of each type of scam to protect ourselves from each of them? What about newly emerging scams, and those that will be invented in the future?

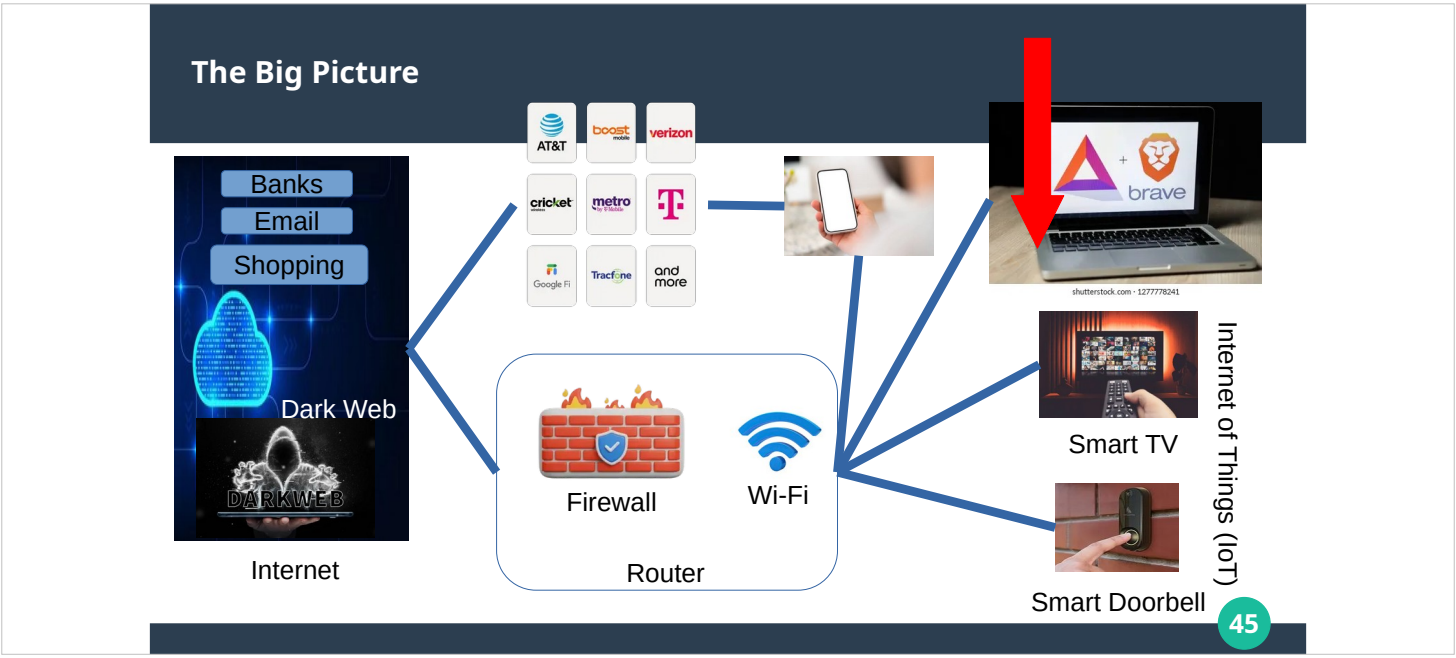
Thankfully, the knowledge we already have can be distilled into just a few important points that will help us protect ourselves from current and future scams.



I came up with this diagram to capture these few important points that we need to keep in mind.

On the left are the websites and services we use on a daily basis, bank accounts we log in into, email accounts we check, basically any and all online accounts we have. We are on the right, the person in front of the computer. In the center of the diagram is the scamming industry. They have already hacked into some of the companies on the left and stolen our information. Over the last 25 years, numerous data breaches have occurred where hackers broke into corporate databases, and copied the personal private information belonging to millions of people. That information is out there for sale on the dark web, shown in the diagram as the filing cabinet. The data breaches that have already happened are marked by the number 1 in the red circle. So we should take it for granted that our information is out there for scammers to use against us. They can and do use this information to target us further. In order to do this they create fake websites that look like the real websites of the companies we have online accounts with, shown to the right of the filing cabinet. The scammer's goal is to somehow get us to go to these fake websites, or perhaps give up our account username and password over the phone so they can profit off of it, either directly by stealing money from our accounts, or by selling the information to other scammers. To this end, they send us phishing emails or call us on the phone. This is marked by the number 2 in the yellow circle. 1 has already happened while 2 is happening now. Everyday. And it will happen tomorrow and every day in the future. Our job is to identify these attempted contacts by scammers, stop engaging with them and avoid doing what is marked as 3 in the green circle, with a red cross below it. We don't want to visit the fake sites nor believe the caller on the phone is a true representative of our bank or utility company. What we want to do instead is number 4 marked in the green circle with a green check-mark next to it. We want to use a VPN which we will talk about in a minute and go directly to the real websites and if we need help, call the real customer service agents at these companies. Our mantra is: Don't call me, I'll call you. Because of spoofing, we can't trust the caller is who he says he is. Hang up and call the customer service number on the website of the company.

If it helps, print out the diagram and stick it on a wall until it becomes a habit for you to question incoming attempts to contact you whether it is over the phone, email or text.



There are a couple more things we can do to protect ourselves from cyber-scams.

These are about strengthening the security settings on our own devices, so we can be confident that we're protected. With this confidence, we're less likely to believe a pop-up declaring we have a virus on our computer, or a scammer on the phone trying to convince us we're somehow in trouble. We go back to our big picture diagram and look at our computer to see what we can do to protect it.

This is marked by the red arrow at the top left of the diagram.

Computer/Laptop Security

Computer and laptop security.

Desktop computers and laptop computers are similar to each other while smartphones have a few commonalities with computers but are different in some respects.

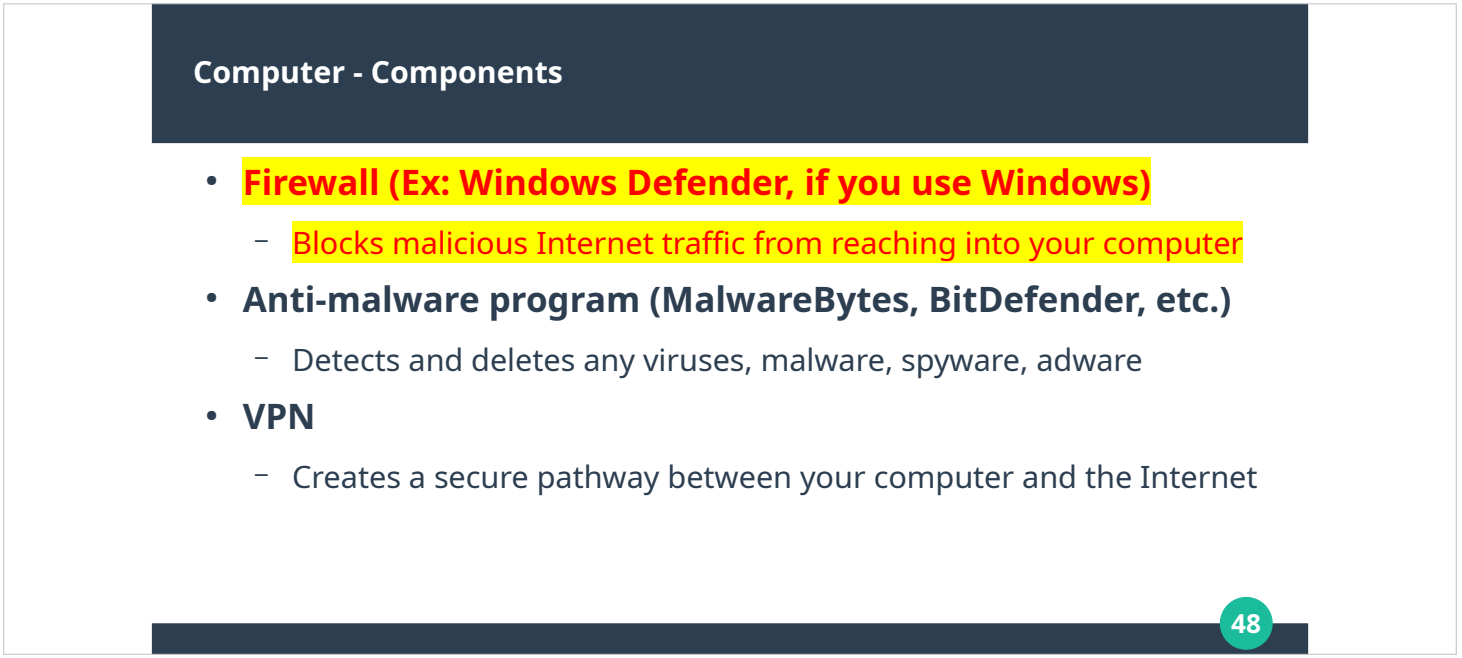
In this presentation, we go over computers and mention smartphones where they are similar, but in the next presentation, presentation 201, we cover smartphone security more in-depth.

There are three main components here and we will go over each in the next few slides.

We have the firewall.

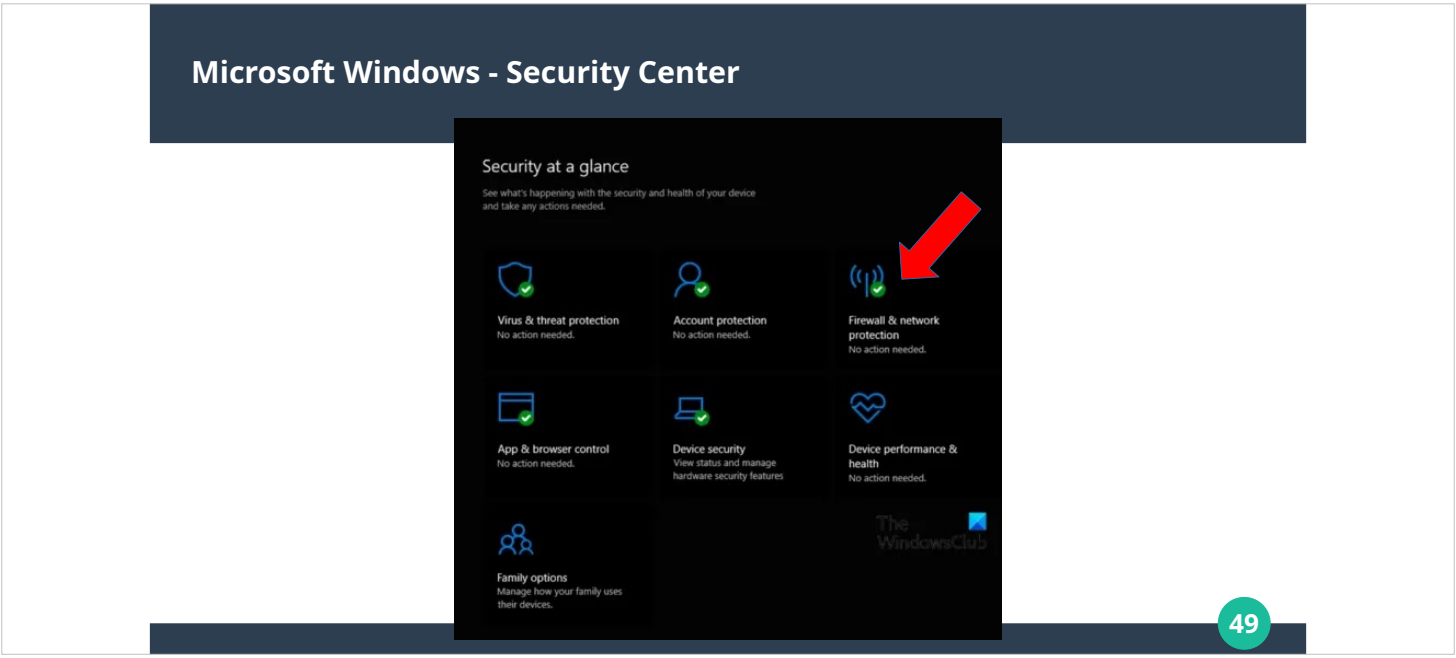
Then we discuss anti-malware software that we can install on our computer.

And I introduce Virtual Private Networks (VPNs)



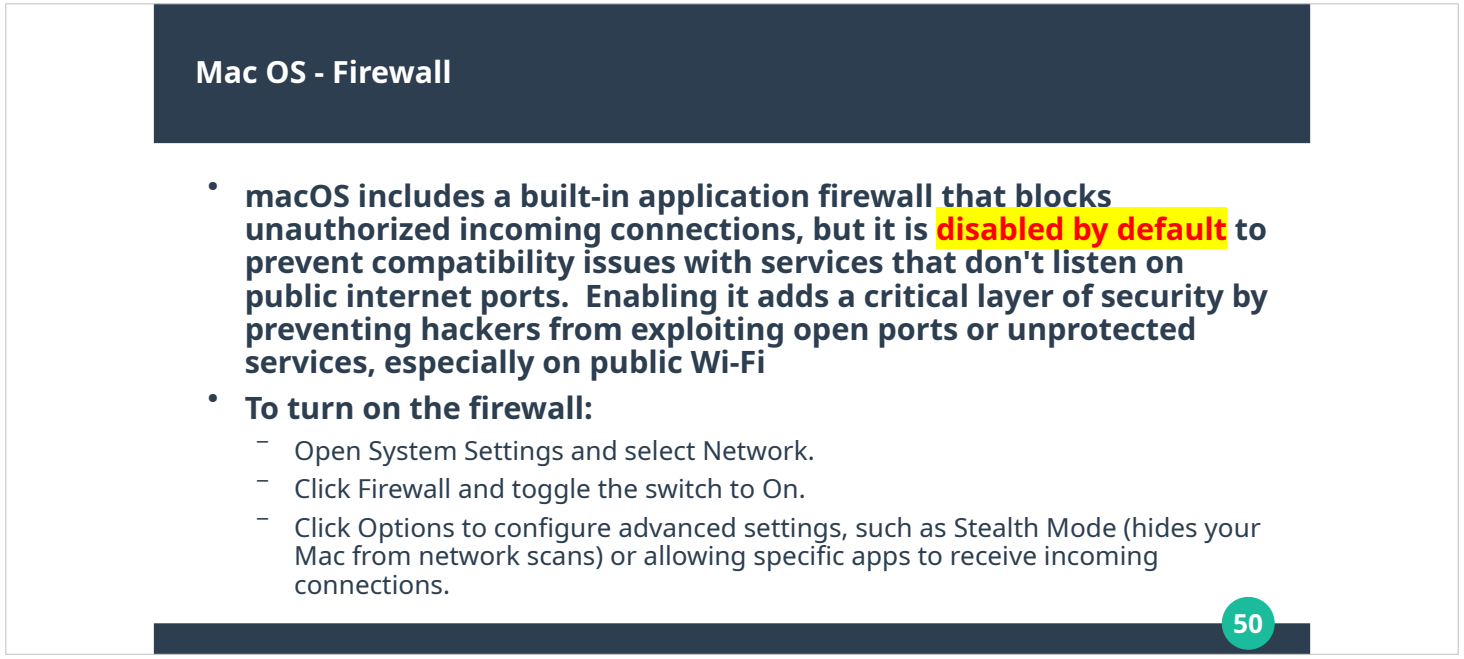
What's a firewall? Think of it as a barrier, a wall or fence that keeps unwanted things from coming inside your home. A firewall blocks incoming traffic from the world "wild" web from entering your computer. We can define rules on exactly what kind of traffic from what sources we want to block, or we can simply block all incoming traffic, which is the default setting when a firewall is enabled.

Essentially, all we need to make sure is that we have a firewall installed on our computer, and that it is turned on and enabled at all times, even when we're not using the computer.



If you use Windows, it comes with a firewall installed straight from Microsoft and it's good enough for our purposes. All we need to make sure is that it is enabled.

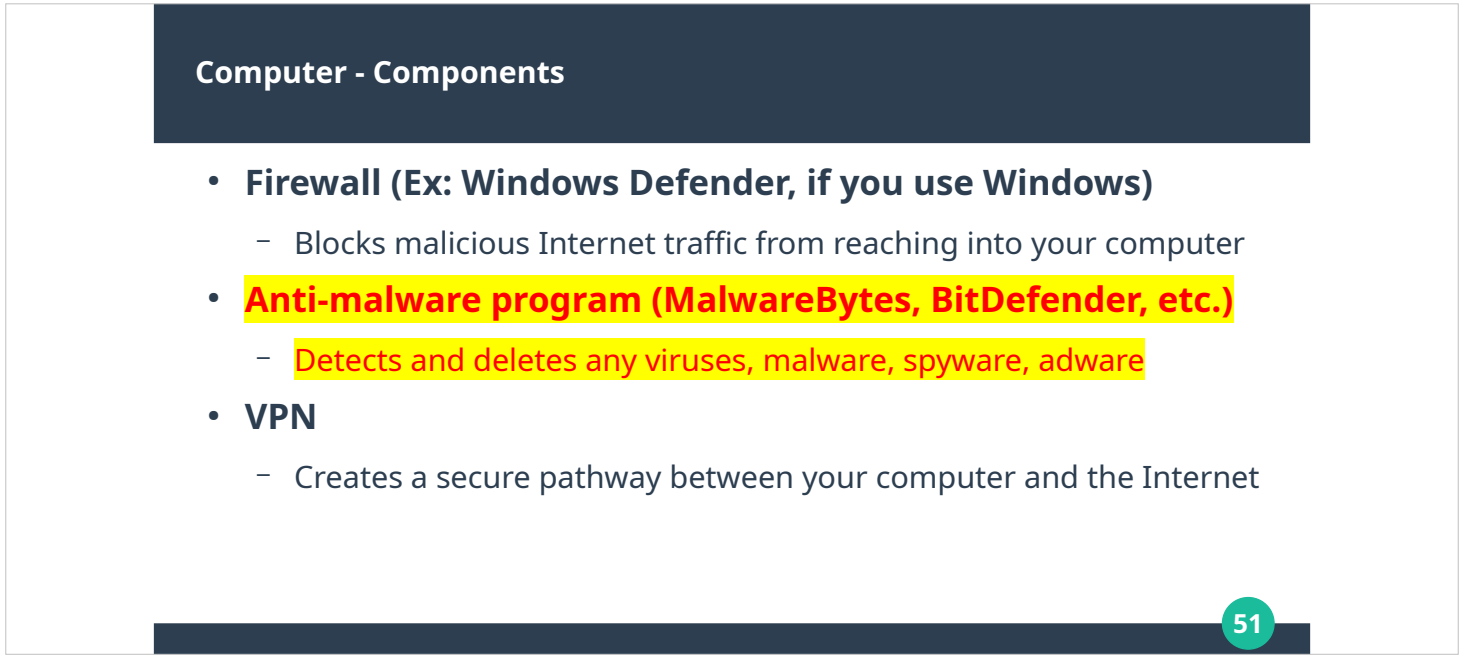
To do this, we go to the Security Center and look for "Firewall and Network Protection" and make sure there's a green check-mark on it. If it's not enabled, there should be a button that says "turn on". Just click on it and the check-mark should appear.



On a Mac, the firewall is installed but disabled by default.

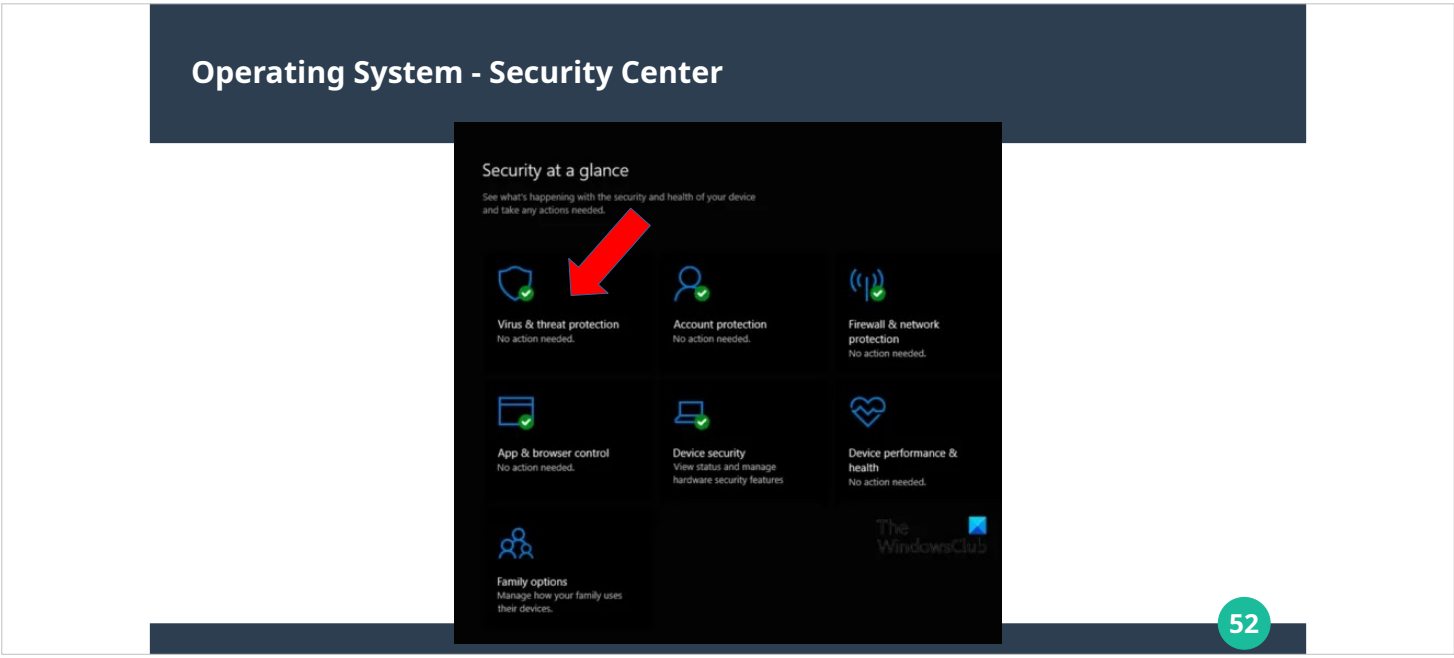
To turn it on, open “System Settings” and select Network. Click “Firewall” and toggle the switch to On.

On smartphones, firewall technology is directly built into the system so we don’t need to do anything to turn it on.



For our purposes, the terms malware, viruses, worms, spyware, trojans, adware, all mean the same thing. It's any unwanted piece of software that is running on our computer, whether it was installed without our knowledge by someone else, or we downloaded it ourselves not knowing it's bad for us.

Malware can do all sorts of things. They can record every keystroke, every website we visit, the passwords we enter there, and send all of it to a scammer sitting on the other side of the world. They can also turn off security features like firewalls and anti-virus programs, making our computers more vulnerable to more malware. Malware can show fake error messages, or crash our computers, and then ask us to call a number to fix it. Malware can display spurious messages asking us to download programs that will clean our computers, which if we do, is basically akin to opening a backdoor for more malware.



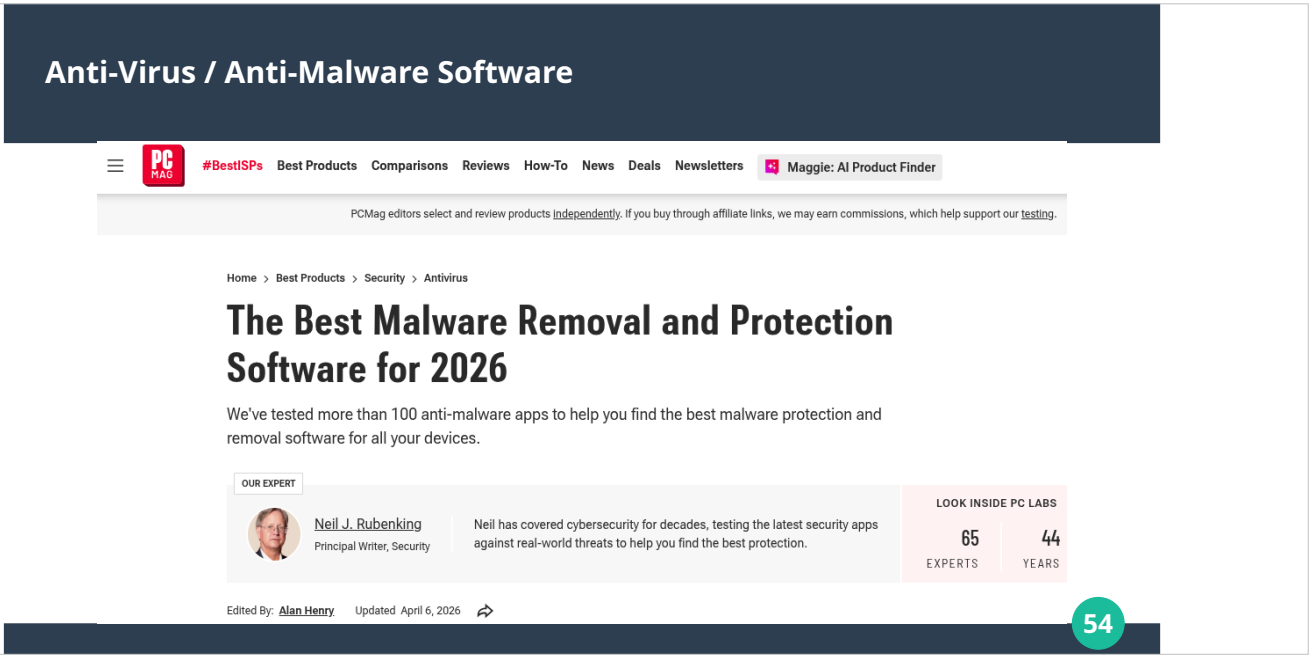
Windows comes with a built-in anti-virus program called Windows Defender that we just need to enable. Again, we go to the Security Center, and make sure there is a green check-mark on “Virus and threat protection”. In general, all the items in the Security Center should have a green check-mark.

Back in the day, Microsoft didn’t include any anti-virus with Windows and we needed to purchase our own from companies like McAfee, but now Windows Defender comes installed and enabled by default. We just want to double-check that it’s always on.

Mac OS - Anti-Malware

- **While macOS includes built-in security features like Gatekeeper and App Review, they lack real-time malware scanning and advanced ransomware protection, making third-party antivirus software advisable for full safety**
- 

On Macs, the features that come from Apple are not comprehensive so it's advised that Mac users install a third-party anti-virus program.



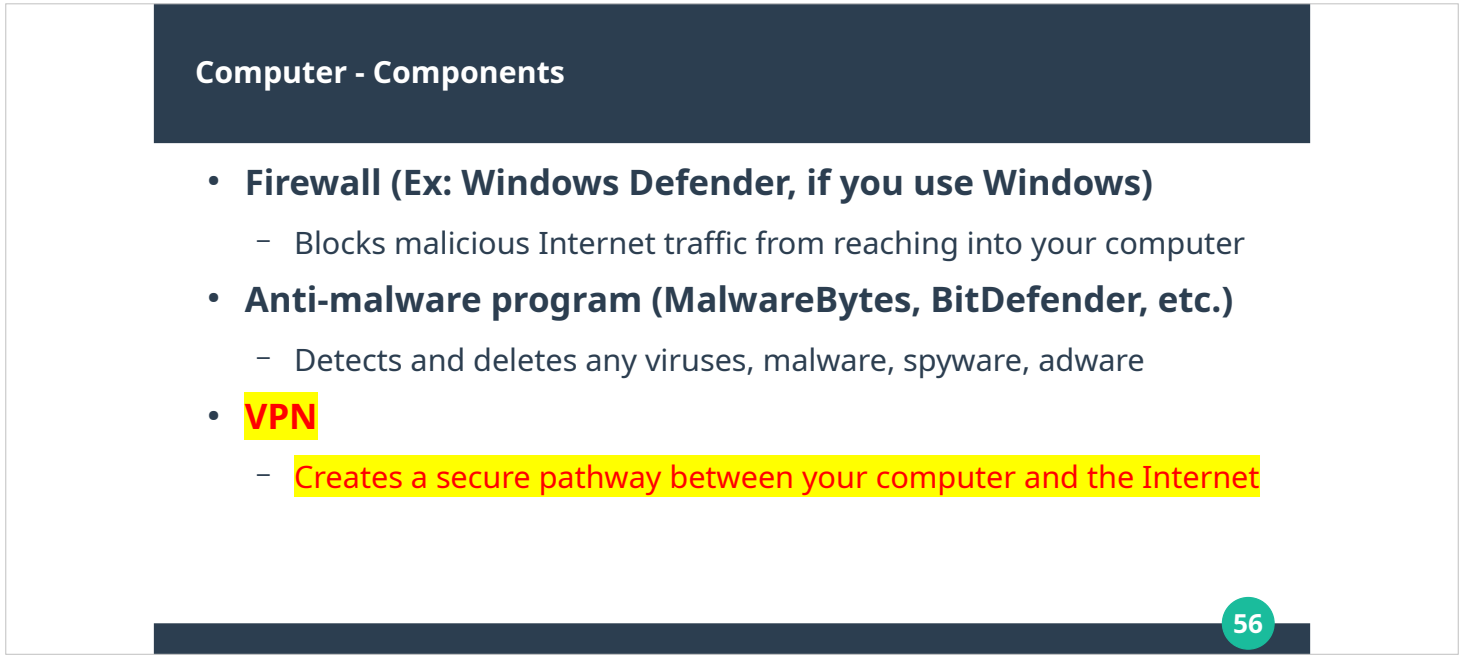
There are several good independent review sites online that compare some of the leading anti-malware programs and rank them. Here's one such review from PC World. Take a look at the comparison, prices and other factors and based on your needs, pick one to try or buy.

When you install an anti-malware program, Windows will recognize the new program and use it for anti-malware protection in place of Windows Defender.

Here's another review site called CNET, which is a leading computer industry publication

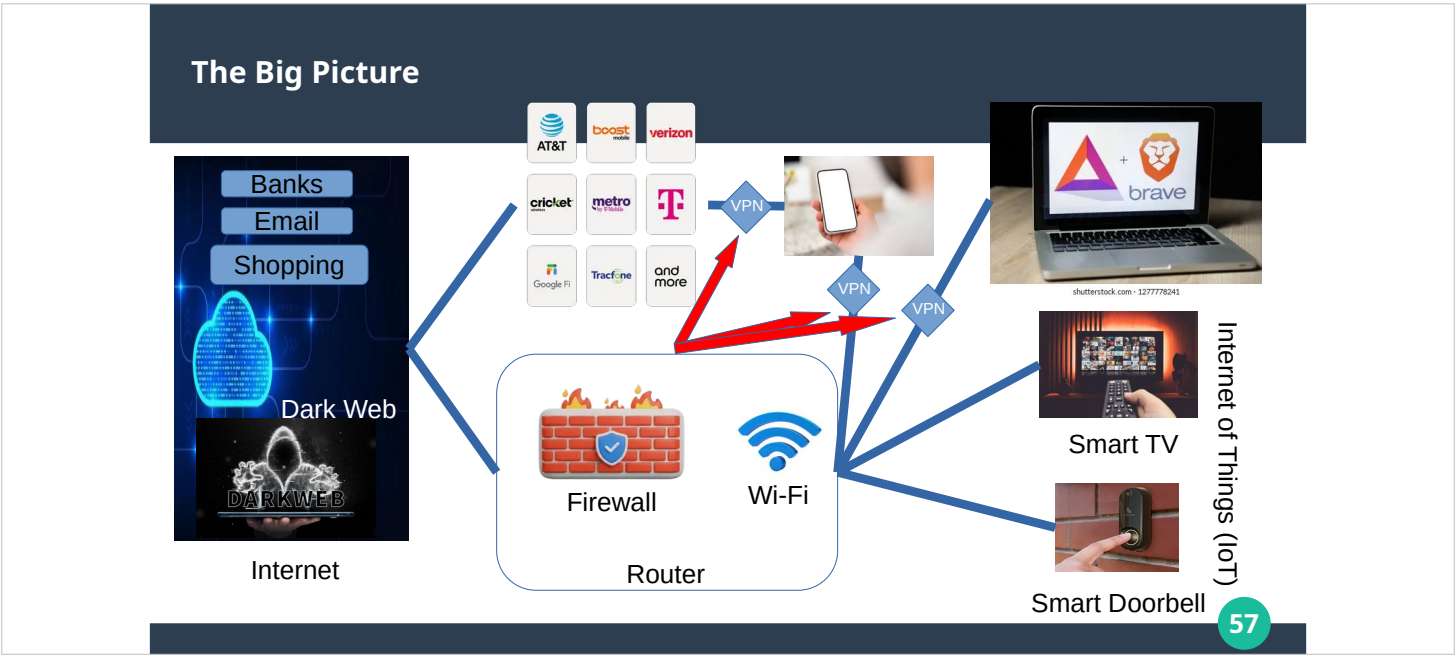
Smartphones could also use anti-malware programs because some of the apps we install tend to be malware. Anti-malware programs on smartphones scan all the installed apps and alert us if something looks suspicious.

Typically, when you buy one of these, multiple devices are included in the subscription package but make sure to double-check based on your needs. Also, there are savings if you buy a family plan that covers everyone and all their devices.



The third component to secure your computer, and for that matter, your smartphone too, is a piece of software called a Virtual Private Network, or VPN for short.

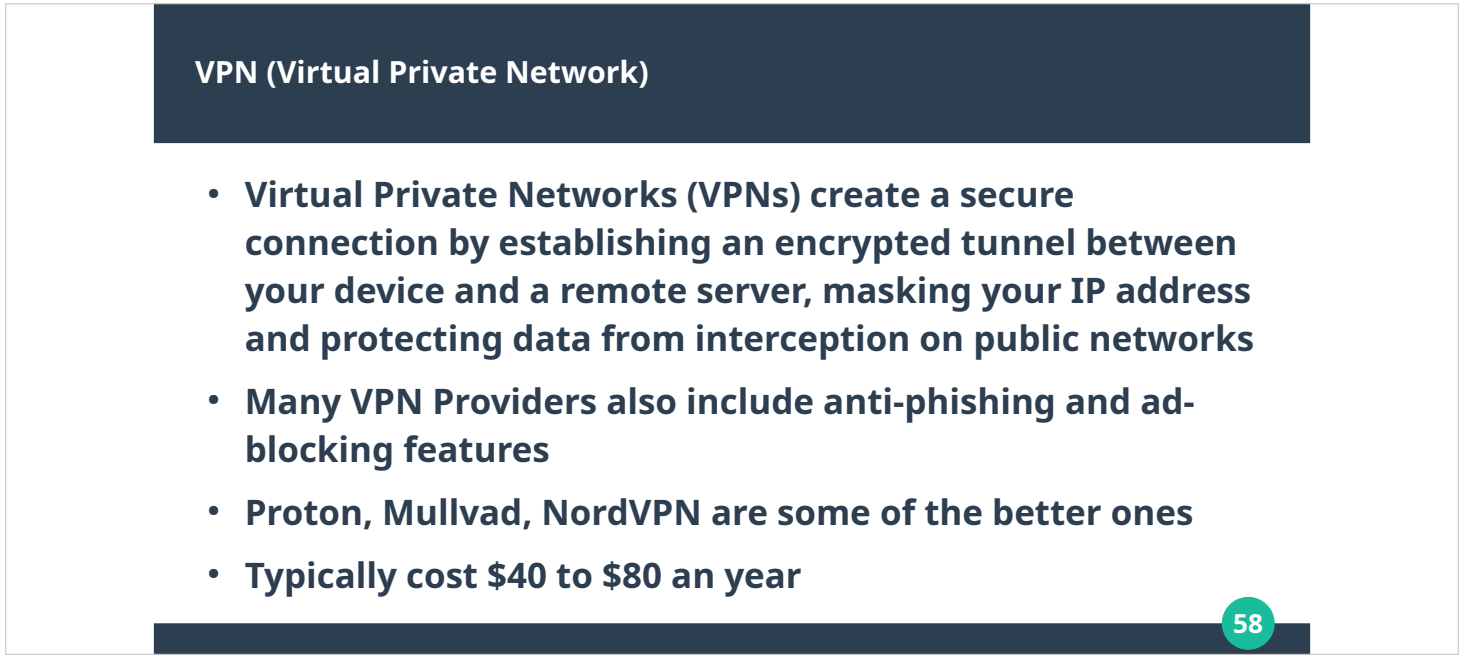
It may sound technical but it’s really easy to install and operate.



When we look at the big picture, so far, we talked about the Internet on the left, and our devices on the right, but haven't said anything about how the devices connect to the Internet, the pathways the traffic follows between the source and the destination.

These pathways are pointed to by the red arrows in the picture.

A VPN does two things. One is it secures these pathways. Traffic between your computer and your bank , for example, is encrypted and not visible to anyone watching the network. Who could be watching and what could they do with this information? If you're in an airport or a coffee shop connected to the Wi-Fi they provide, it could be anyone else connected to the same Wi-Fi who could be snooping in. Or it could be the company that provides our home internet service, or our cell phone company. They could sell our information to the highest bidder. A VPN garbles the traffic so no one but us and the bank or the email service we use can read it. Our traffic remains secure.

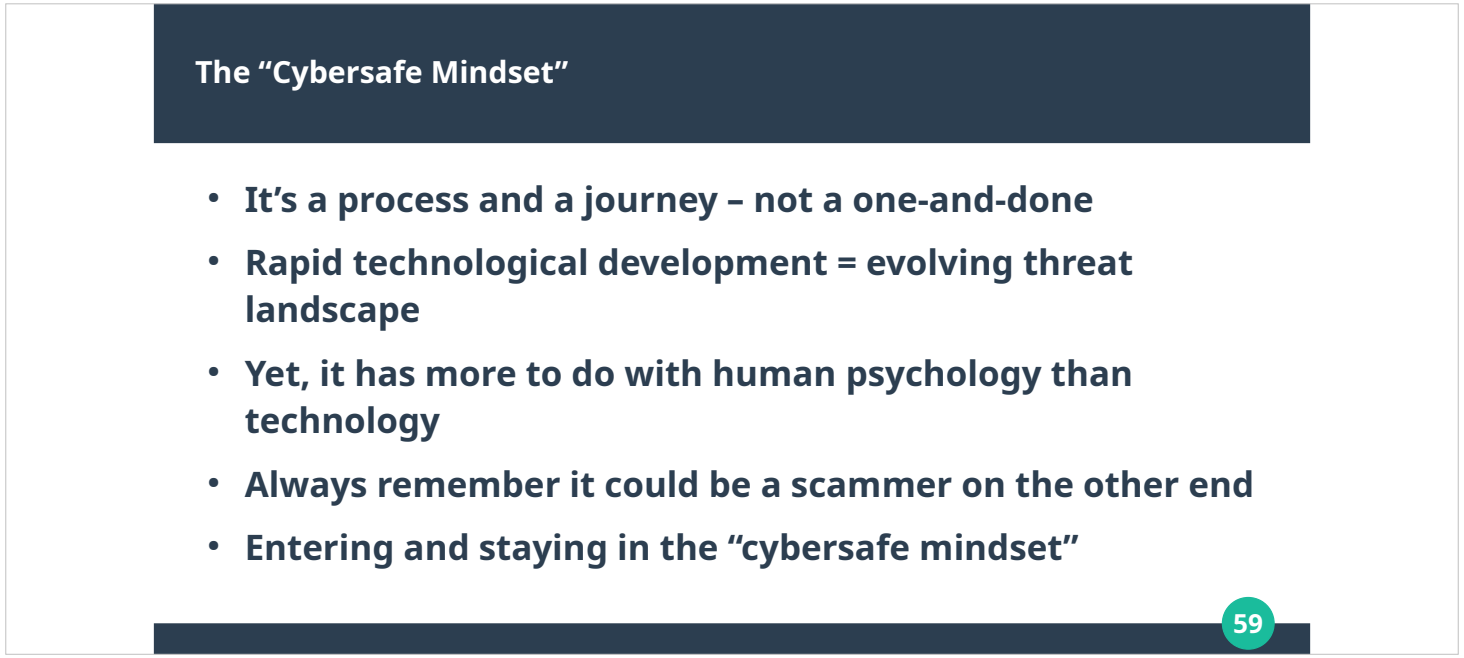


The second feature a VPN provides is increased privacy. Imagine giving out your home address every time you visit a store or a restaurant. There's no reason to. That information could be misused by a store employee or someone who happens to overhear you.

But on the Internet, we have to provide a return address so we get a reply back to whatever it is we want to do – say, make a bank transaction. A VPN provides us with the equivalent of a PO Box, so when we mail a postcard, we mention the PO Box number as the return address, instead of our home address. The reply is sent to our PO Box and our home address remains private. The bank already knows our address, but none of the many other sites we visit to check the news or the weather need to know our home address. So a VPN preserves our privacy and also improves security. Increased privacy is improved security.

Most VPNs also provide additional features like anti-phishing and ad-filtering. Some also warn about sites with known malware on them. They cost $40 to $80 for an yearly subscription and are worth it the benefits they provide. Family plans cover everyone and multiple devices and computers.

Some good VPN providers are Mullvad, NordVPN and Proton VPN.



We’re almost done with the presentation. I want to talk briefly about what I call the “cybersafe mindset”. We have to understand that cybersafety is a process and a journey, not a one-and-done deal. It’s a methodical marathon rather than a single sprint. It’s about slowly getting into certain good habits and making them second nature, like defensive driving.

No matter how much technology changes on us, no matter how much AI advances, it ultimately comes down to human psychology that tends to be the weak link that scammers are looking to exploit. Developing good habits like keeping our devices updated and secure, realizing and accepting the fact that our names and email addresses are already out there, learning about common pitfalls and traps and staying alert and skeptical, all help us stay safe.

Always remember, it could be a dog on the other end of the phone line!

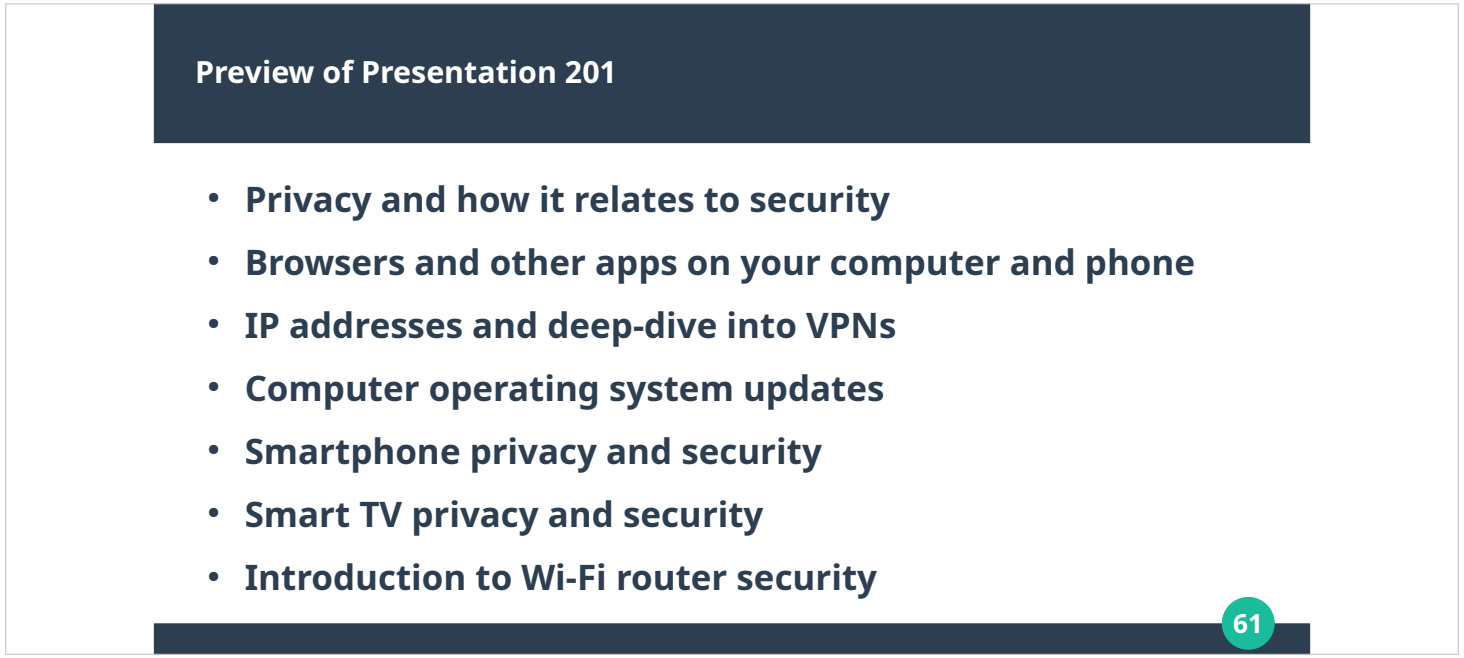
The website where you can find all the slides shown in this presentation is LakelandCybersafe.org (one word, no space or hyphen. And it's .org not .com) There are dozens of articles and videos in the Resources page there.

Some other good resources online are securethevillage.org where there's a section for individuals.

There are many government websites that have lots of good advice. If you're a senior, sign up for the newsletter at Operation Senior Shield which is a program run by the Florida state government.

There is secureflorida.org with a ton of information for individuals and families to stay safe online.

The Polk County sheriff's office has some resources as well on their website.



This is an outline of what we go over in the next presentation, presentation 201.

Privacy and its relationship to security

Browsers and other apps on your devices, and how some browsers can be better than others in terms of privacy and security.

We dig more into VPNs and how they work. And why it is a good idea to mask our IP address.

We see how to keep our devices and computers up-to-date.

And how to improve privacy and security on our smartphones.

We learn how our smart TVs spy on us and how to prevent it.

Finally, we end with an introduction to routers and Wi-Fi security.

Thank you for taking the time to be here.

If you're new to much of this content, I hope you feel inspired to take the next steps to begin your personal journey on the road to having a strong online security posture.

If you're already familiar with many of the things we discussed in this presentation, consider attending the next one where it gets a little technical but still remains in the category of "essential things to know" as you enhance your knowledge and understanding.

Thank you, again!