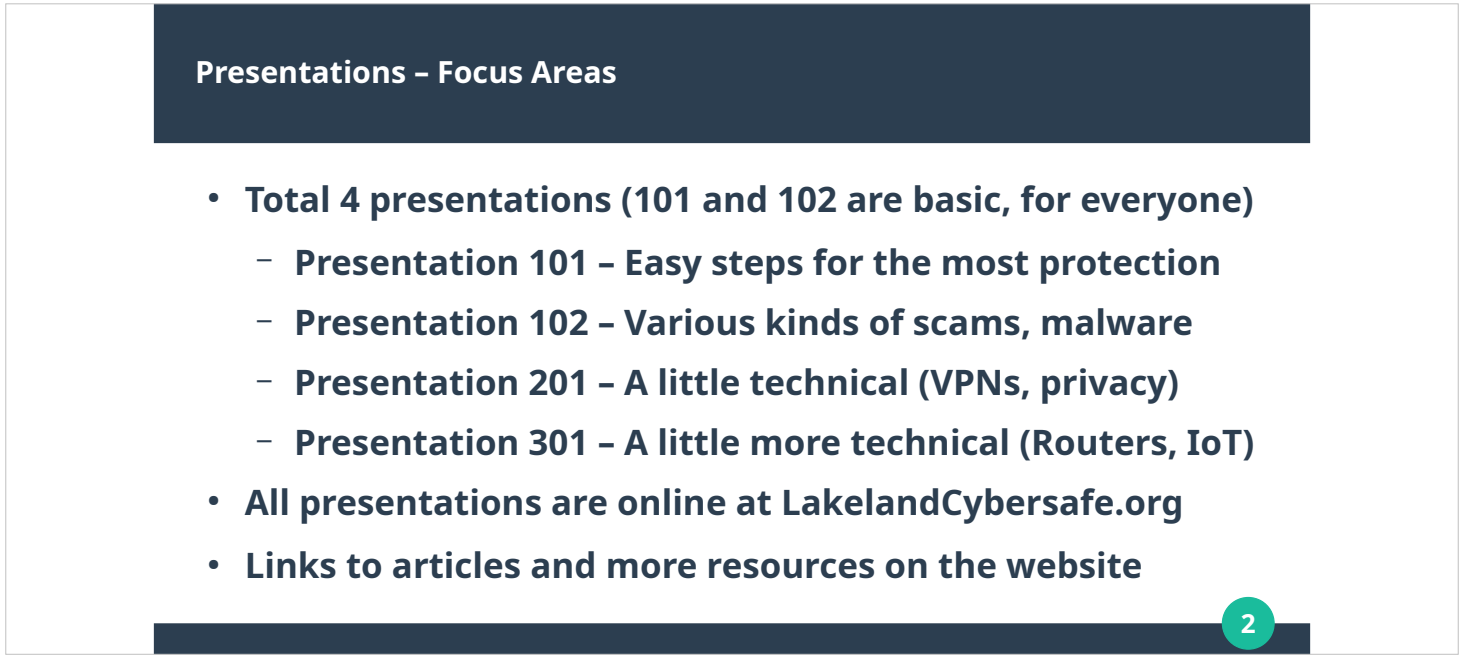

Thank you for being here today for this presentation on cybersafety.

Imagine you're traveling to a foreign country. You do some research on which places to visit and where to stay. You may not want to venture into some of the rougher areas of town and might plan your day so you're not out too late at night in areas you aren't familiar with.

The Internet is a little bit like that. It has its seedy corners that the normal web surfer doesn't visit, or in many cases, not even be aware of. But unlike in a tourist spot, on the Internet, it's harder to tell what's real and what's not, what's safe and what's a risk. We need to develop a sixth sense.

Cybersafety is about exactly this – how to be street smart on the world "wild" web. It's learning what to avoid. And we know what to avoid when we develop a keen eye for detail. This presentation will help you develop habits to navigate the Internet with confidence and discernment.

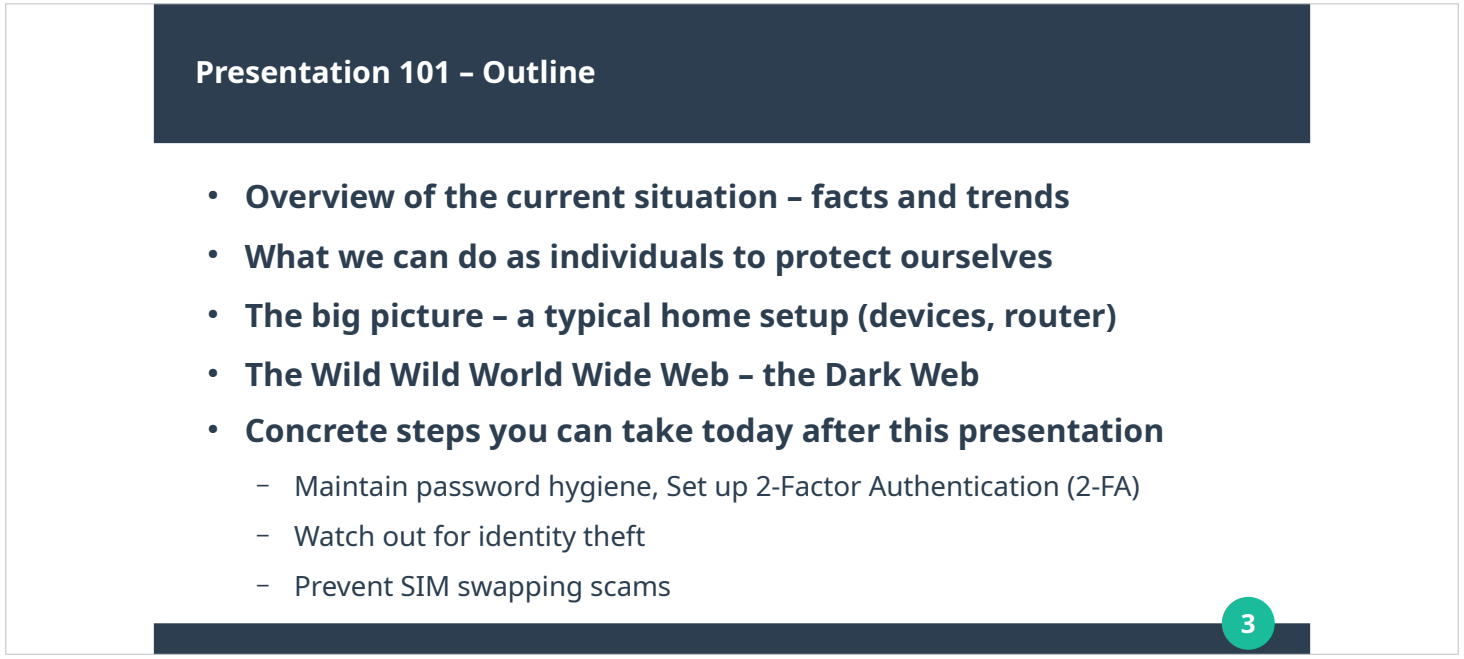



There are a total of 4 presentations. The first two are basic and are meant for everyone. If you use the Internet, check email, watch Netflix or shop online, you already have the skills to understand everything in the first two presentations. This presentation is the first – presentation 101, where we talk about some key cybercrime trends and statistics before going over some practical information that will help you navigate the Internet more safely. For our purposes, cybercrime, cyber scam, and cyber fraud all mean the same thing.

We go deep into various types of cyber scams in the second presentation, presentation 102, where we'll also look at the common themes and patterns in many of them, that once you learn to identify, will help you spot any potential scam attempt and stop it in its tracks.

The third presentation in the series, presentation 201, 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, presentation 301, is about routers and other more technical measures that build upon the ideas discussed in the first three presentations and helps you secure your entire home network for you and your family.

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




While we start out this presentation with some data and statistics on the cybercrime industry (and it is happening on an industrial scale), and learn about the shady corners of the Internet called the dark web, much of it is about practical steps you can take to protect yourself and your family.

You may already be doing some or many of these things without realizing how they connect to the overall picture so we will put things in context with a diagram of the typical home network including the router and all your computers and devices. We will use this setup as the common thread connecting all the 4 presentations and revisit it many times.

We will talk about password hygiene, 2 factor-authentication, and ways to prevent identity theft. We also learn how to reduce the possibility of becoming a victim of a particular scam called the SIM swapping scam.

When we're done with this presentation, you will have a small list of things to do that will set you up on a safe foundation. You will have looked at some of the easiest things anyone can do with the most impact on their security posture.

## 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.


Cybercrime affects individuals, families, and businesses of all sizes. It can paralyze entire organizations and institutions, federal government agencies, city governments, utilities, hospitals, and even non-profits.

Large organizations spend billions of dollars every year on training for their employees, and on technology for their IT staff, which is tasked with protecting the organization from hackers and cyber criminals. Many organizations have a dedicated security department, headed by a Chief Information Security Officer. Such a department has access to a multi-billion dollar cyber security industry that puts out reports like the one shown here – detailing key current trends and the measures to deal with them. We have much to learn from such reports.

It's a cat and mouse game between the criminals and the cyber security industry that is always trying to keep up with the latest innovations that the criminal mind dreams up. AI has only raised the stakes in this evolving battle.

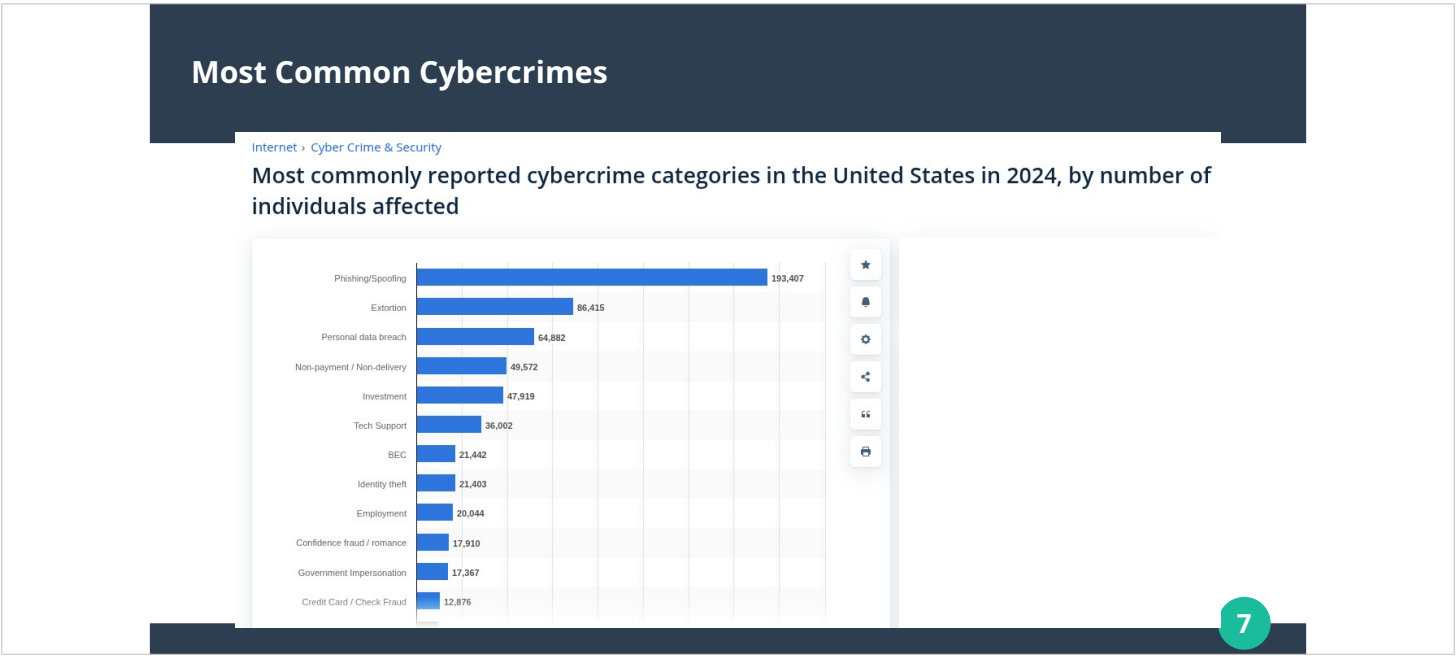

If we took all the damages that cybercrime causes to everyone the world over, and think of it as the GDP of a country, it would be the third largest country amounting to $10 Trillion.

The Federal Trade Commission received about 6.5 million cybercrime reports in 2024. 40% of them are related to fraud, and 18% to identity theft.

Americans ages 60+ filed 201,266 cybercrime complaints in 2025 and lost $7.75 billion — a 59% annual increase. The average loss per senior was $38,500, with 12,400 losing more than $100,000 each.

The world sees some 850,000 cyber attacks annually. That’s over 2300 attacks every day, or three attacks every two minutes.

With the advent of AI in recent years, this is beginning to increase even more as criminals are figuring out how to automate and deploy all manner of attacks on a large scale. AI has even proven that it can find vulnerabilities that humans can’t.

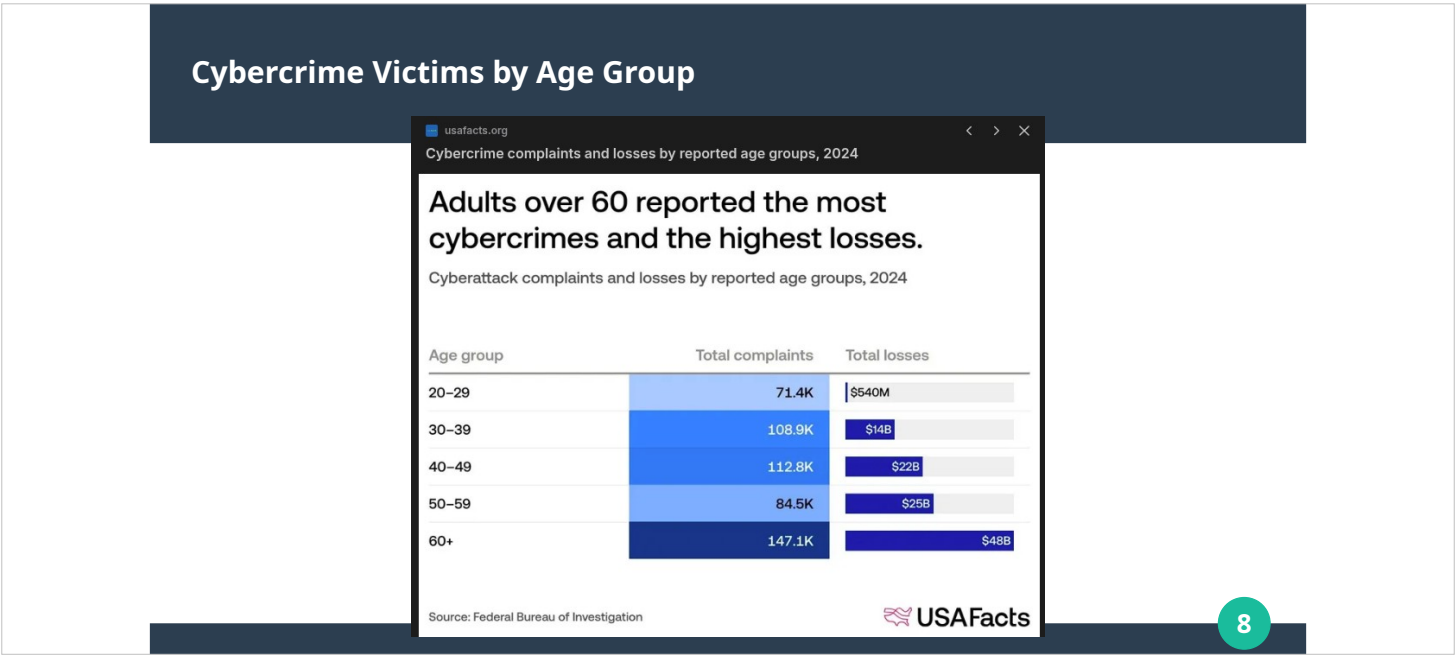



This is a chart showing the most commonly reported cyber crime types in the United States in 2024, going by the number of people affected by each type.

By far, the lion's share of cyber crime is attributed to phishing/spoofing scams. This is essentially trickery where a scammer impersonates someone we trust and leads us to revealing private personal information of account credentials like usernames and passwords.

The other types of cyber scams listed here are extortion or demanding a ransom, personal data breaches or hacking, non-payment/non-delivery (when you order something and it doesn't show up), investment scams like pyramid schemes, tech support scams, business email compromise or hacking into an employee's company email, identity theft or impersonating the victim, employment scams, confidence/romance scams, government impersonation, credit card or check fraud.

We will go over many of these scams in presentation 102.

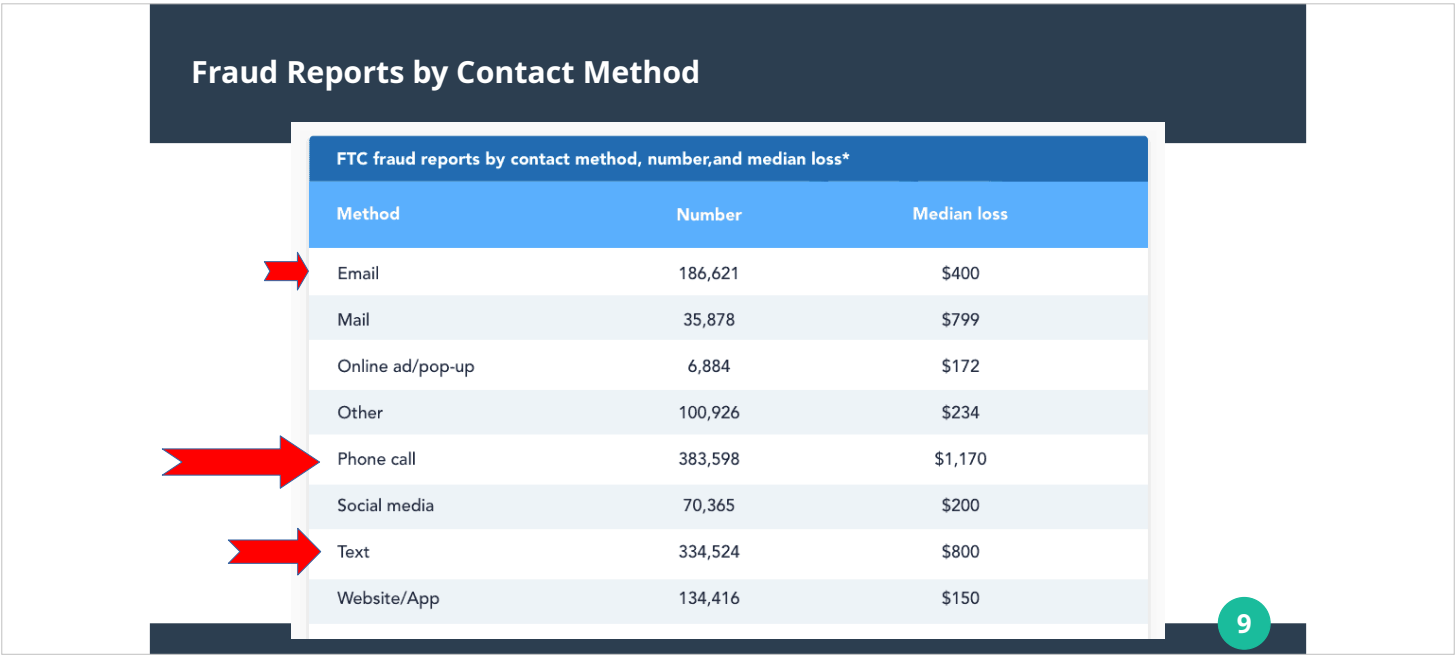



If we look at the victims of cyber crime by age group, adults over 60 reported the most cyber crimes and the highest losses.

Adults over 60 reported 147,000 cases amounting to a total loss of $48 billion in 2024.

As we see in the chart, the losses decrease with age, possibly because younger people have fewer assets, but also because they might be a little more tech-savvy. However, even the youngest group (ages between 20 and 29), still lost $540 million. If we divide that by the number of complaints they filed, which is 71,400, we get $7,500 per complaint. So we see that the youngest among us who grew up with the Internet still fall prey to scammers, because ultimately, it comes down to human psychology and it’s basically the same across all age groups.

Cyber crime does affect senior citizens much more and my hope is that by becoming aware of how scams work, all of us here and the residents of Lakeland will be one step ahead of any attempts to scam them.

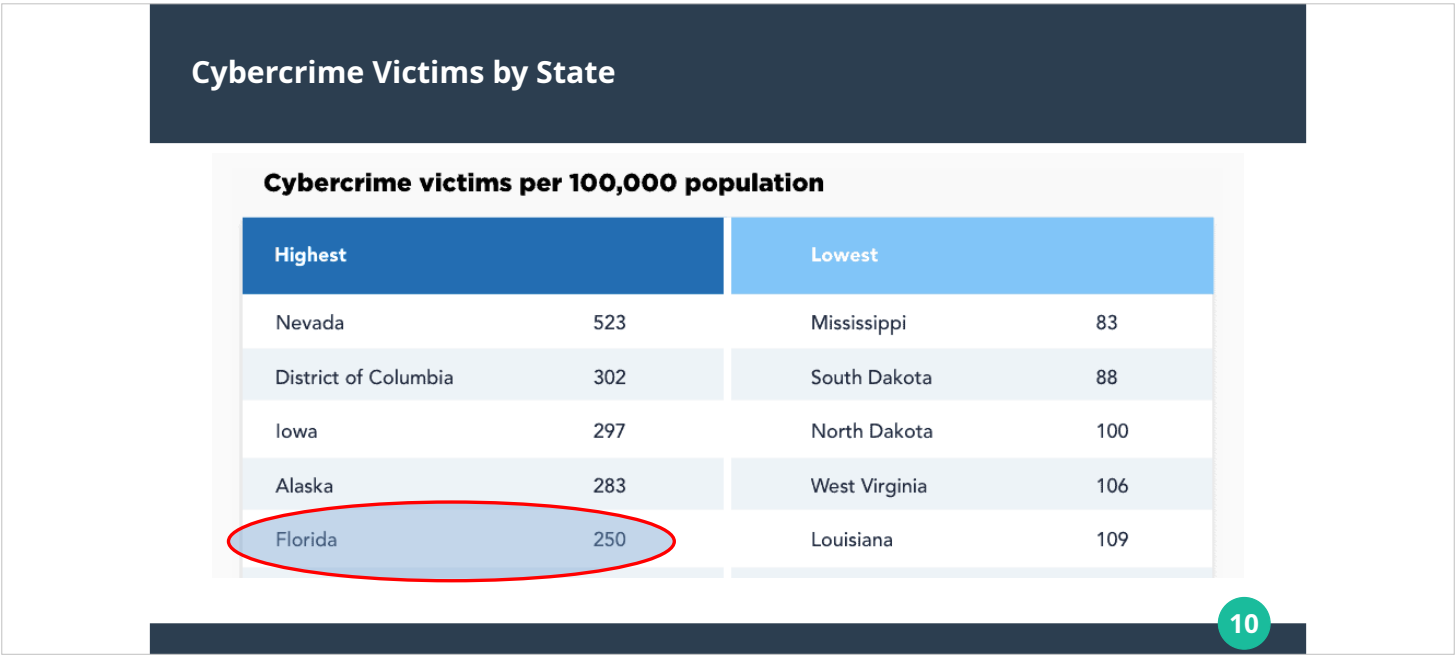



Let’s take a look at how these scams start. It turns out that the highest number of cyber scams start off when we pick up our phones to answer a call. This old-school method is the most effective for a scammer to sound personal yet authoritative, even as he impersonates someone we trust, such as a bank employee.

The next highest is text messages. Though not as personal, a text message is still very effective because a scammer can send a lot of them in one go and see who bites.

Email is next and is even cheaper to send to thousands of people in one go. It’s like casting a large fishing net into the ocean. They’re not targeting any specific person but simply wait and see who responds, so they can then target them one by one.

So even though the phone is number one on the list, an email or text that we responded to previously might have helped bring about that phone call. The other contact methods on this list are scam web sites and apps, social media, online advertisements and pop-up messages, and regular mail.




When we rank each of the 50 states in the country by the number of cyber crime victims per 100,000 people, we get these two lists at the top end and the bottom end.

On the left, we have the top 5 states with the highest number of victims. Unfortunately, Florida appears in this list at number 5. We have 250 victims for every 100,000 people.

Estimates like these are vastly under-reported. Research has shown that only about 15% of cyber crimes are reported to authorities. The true number for Florida is closer to 1500 per 100,000 people.

To place that in context, Lakeland has a population of about 100,000. So every year, we can expect 1500 Lakelanders to become victims of cyber crime.

My hope is that, with a little more awareness, we can reduce that number down in Florida to the same range that states like Mississippi and Louisiana have. A list of these states is shown on the right of the table.


With the rise of AI in recent years, cyber crime has gone “industrial scale”. It’s become an organized crime where it’s not the lone computer nerd sitting in a basement hacking computers, but large organizations with their own HR departments, recruiting, training, commissions, the whole setup.

An estimated 3.4 billion phishing emails are sent on a daily basis, with over 82% of them generated by AI. AI is also being used to clone our voices, images, writing styles and to even clone our appearance on video calls. The participants on a zoom call believe it’s their boss asking them to transfer funds while in reality, a scammer used AI to create a live impersonation of the boss giving instructions.

While money is the main goal of scammers, some have been seen on social media bragging about their exploits to fellow scammers. It’s become an issue of peer prestige.

While government agencies, law enforcement, companies and institutions like banks are doing what they can to protect us on a daily basis, it is up to us to understand those protections and take responsibility. For example, if we get a phone call and the scammer asks us for our one time pass-code, and we give it to him, and he then uses it to log in into our bank account and steals money, the bank can’t do anything about it.


Efforts are ongoing at multiple levels of government to protect us all from the dangers of cyber crime.

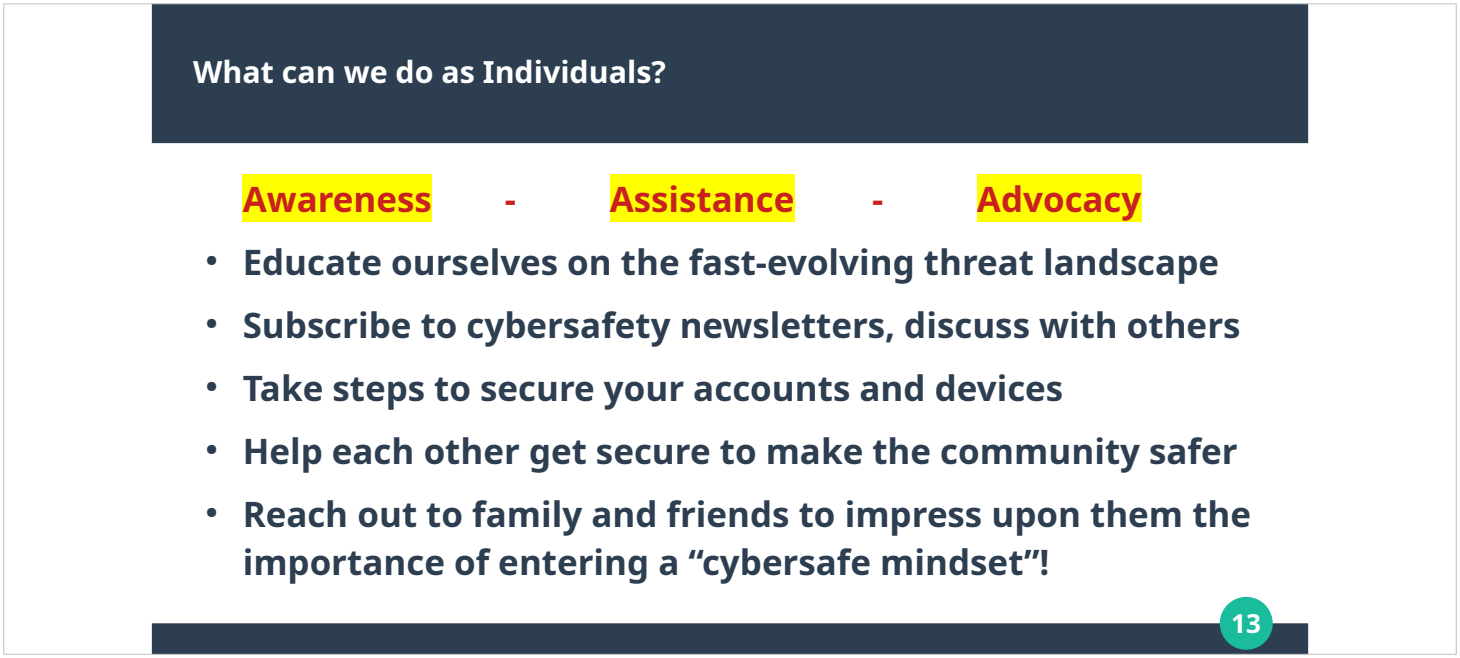
At the Federal level, agencies such as the FBI, FTC, FCC, and the Justice Department have resources for us to learn about scams and fraud, and if victimized, report the fraud at the FBI's Internet Crime Complaint Center (IC3).

At the state level, the Florida Department of Law Enforcement's Computer Crime Center works to educate residents of the state and to enforce the law.

At the county level, the Polk County Sheriff's Office launched an AI Investigative Unit in June 2024. Among other things, they investigate cyber harassment, identity theft, extortion, and deepfake misuse.

Finally, at the city level, the Lakeland Police Department's General Crimes Unit investigates local computer and Internet related theft and fraud.

There are also numerous non-profits and other institutions working in the area of cyber safety that have very helpful resources online.




So what can we do as individuals and families?

We can educate ourselves on the fast-evolving threat landscape, especially with AI added into the mix.

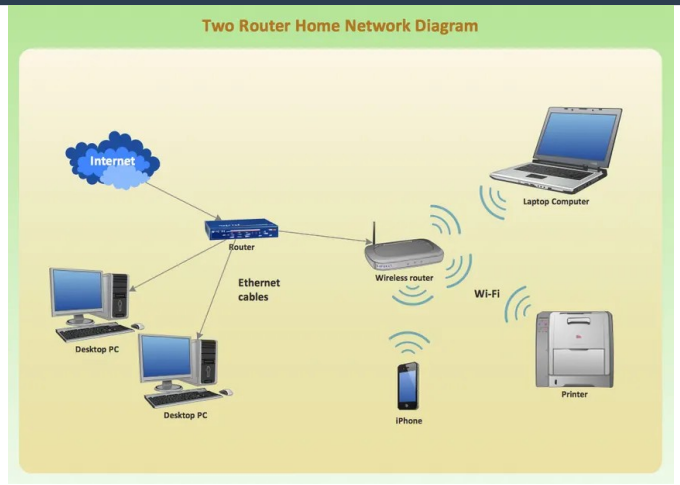
In this regard, subscribing to cybersafety newsletters, participating in cybersafety discussion boards online, or simply talking with each other about this topic helps a lot.

We can secure our online accounts, computers and smartphones to make them less likely to be hacked.

We can help our parents and older relatives do the same. We put on our own oxygen mask first, and then help others around us.

We can learn about the importance of staying alert and entering what I call the "cybersafe mindset". In the rest of this presentation, we talk about some practical steps that will help us enter this mindset.

## Typical Home Set-up

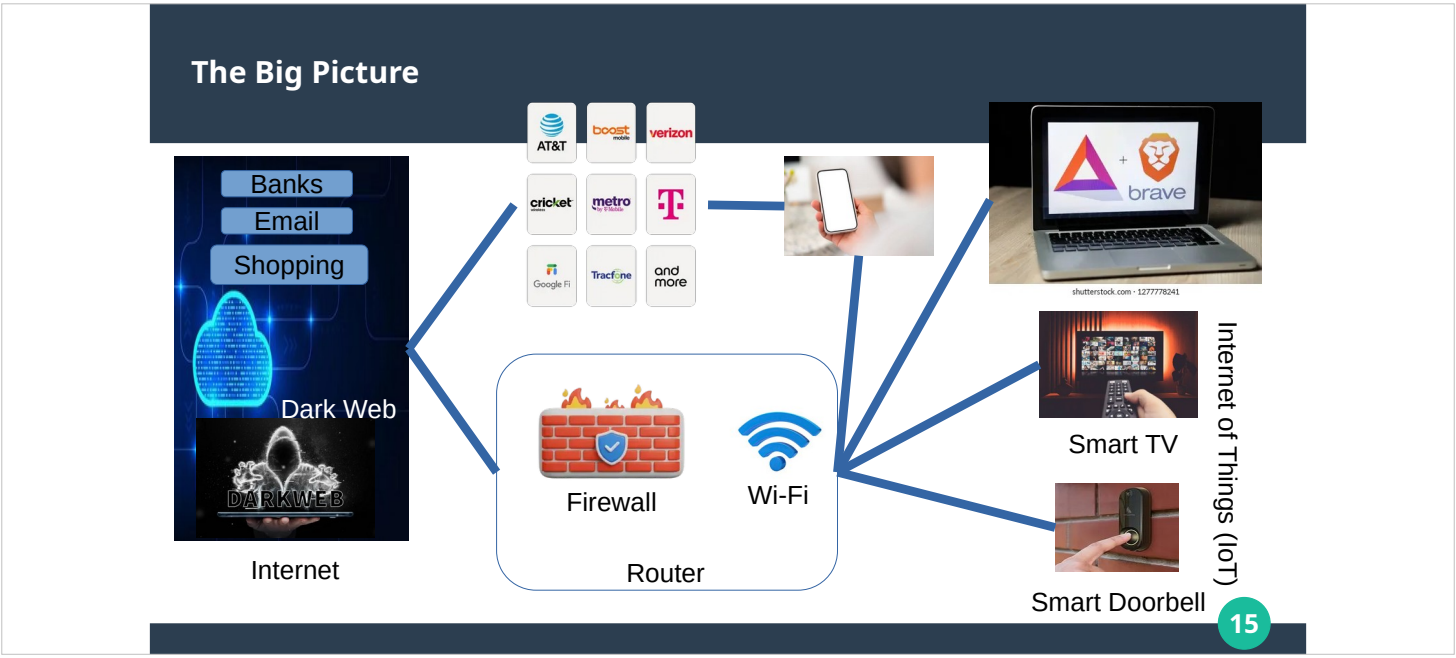



14

Let’s look at how the typical home is set up for Internet. Your situation might vary, but this diagram covers the vast majority of households in America.

At the top left is the Internet, shown as a blue cloud. We connect to the Internet through a modem and a router. Sometimes, they are built into the same appliance, which we will just refer to as the router. If we have a desktop computer or two, they might plug in directly into the router. Or, like our smartphones, we may connect our computers wirelessly to the router using Wi-Fi. Likewise, any other devices we may have, like printers and laptops, connect wirelessly to the Internet through our Wi-Fi routers.

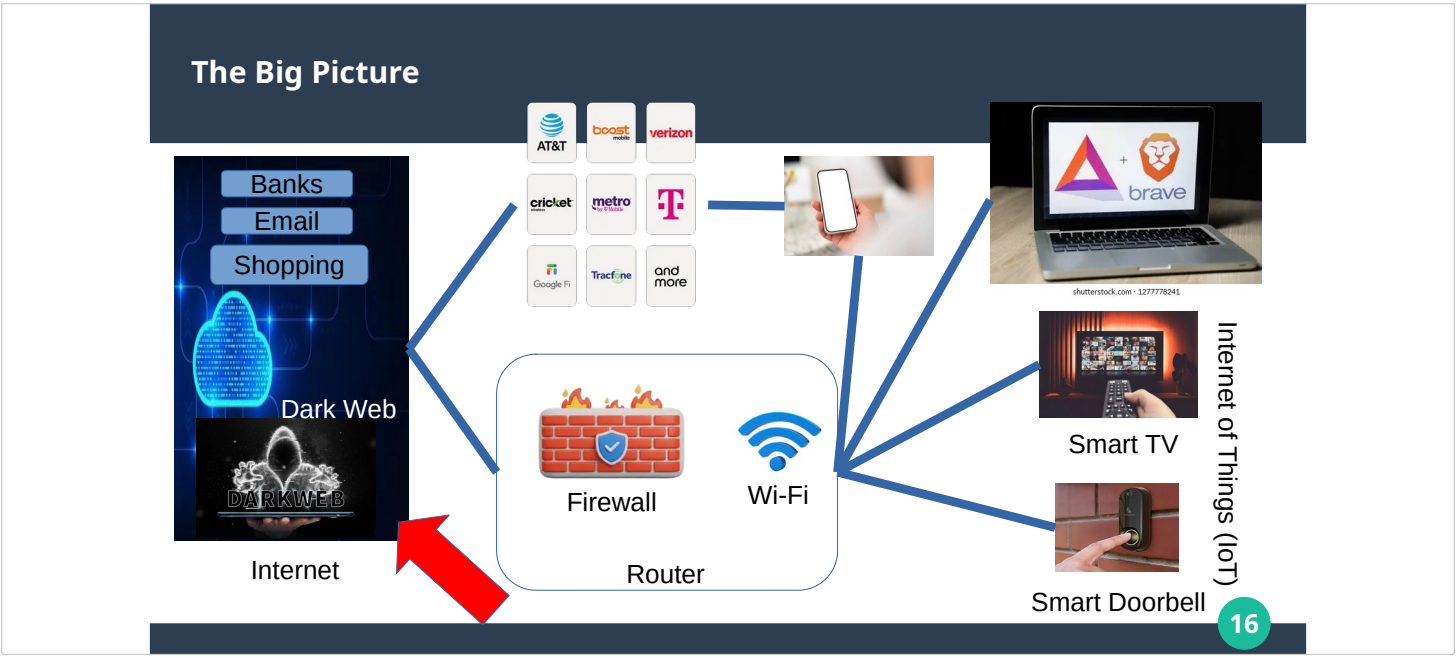
Some larger homes have 2 or more routers, so the Wi-Fi signal reaches every room. These routers talk with each other through what is known as a mesh network. As you move around the house from room to room, your phone might switch from one of these routers to another, so it can have a better signal.




This diagram is essentially the same as the one we just looked at, except that I have added a few more details that are specific to our purposes, so we can focus more on the various aspects of cybersafety.

If we zoom out, we 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. All routers have a built-in firewall that acts as a barrier preventing unwanted traffic from the Internet from coming into our homes. The firewall is discussed in a later presentation.

In the case of the smartphone, when we are not home, we connect to the Internet through the cellular network. This is shown in the diagram at the top, between the Internet and the smartphone. When we're home the same smartphone has the option of connecting to the Internet through the router. The rest of the devices, like the computers (both desktops and laptops) , printers, TVs, smart devices like doorbells, all typically connect to the Internet through the router. The Internet of Things (IoT) refers to such Internet-connected devices as TVs, doorbells, Kindles, etc.




Now that we've looked at the big picture, we're going to focus on the left side of the diagram, pointed to by the red arrow: the Internet and the different parts inside it.

Although frequently depicted as a cloud, the Internet doesn't have much to do with the atmosphere or space. It's all here down on Earth in vast buildings known as data centers. With the rise of AI, the words, "data center" have become a bit infamous for all the damage they do to the environment and water systems. These are AI data centers which are relatively new.

Long before AI came, big companies like Google, Facebook and Amazon have had regular (non-AI) data centers. which actually power much of the Internet we've known. Many other companies also own and operate data centers of all sizes. These are large buildings that contain hundreds of thousands of computers, which in turn, contain millions and billions of pieces of data. This is our data: our money in our bank accounts, our email and text messages, the orders we place on Amazon, the movies we watch on Netflix etc. This is the good part of the Internet.

We also have a part of the Internet that's not so good.

In the next several slides, we talk about how to protect ourselves from the threats originating from this unsavory part of the Internet.

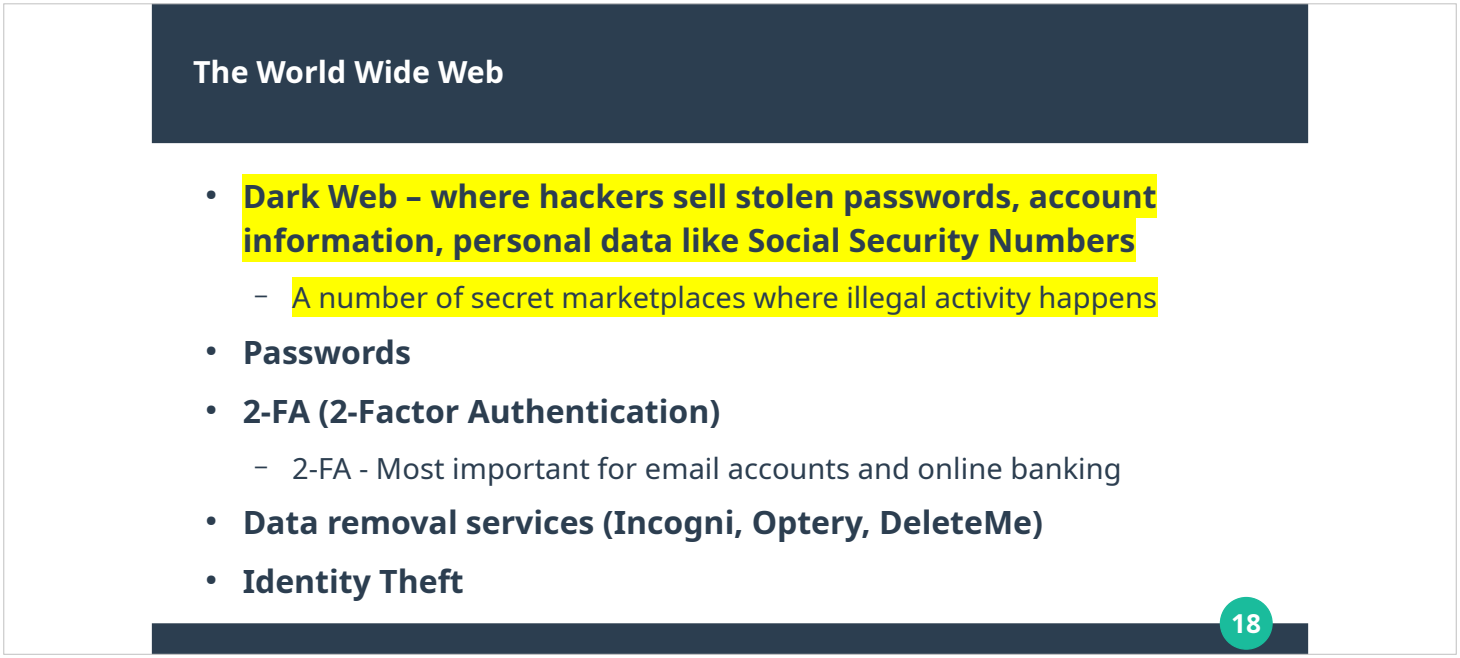

It's called the Dark Web. It's a part of the world wide web, but hidden away from view. We need to understand a few things about the dark web which we will go over in the next few slides.

We will then talk about how to secure our accounts and information online, which are constantly under attack. Everyone has passwords to at least a few accounts, so we will talk about the best way to deal with passwords.

In addition to passwords, important accounts like bank accounts and email accounts, need to be secured with a second form of authentication, which we will look at next.

Our personal information is already out there on the dark web as well as on legal websites that trade in such information. We will look at ways to remove our information from the Internet.

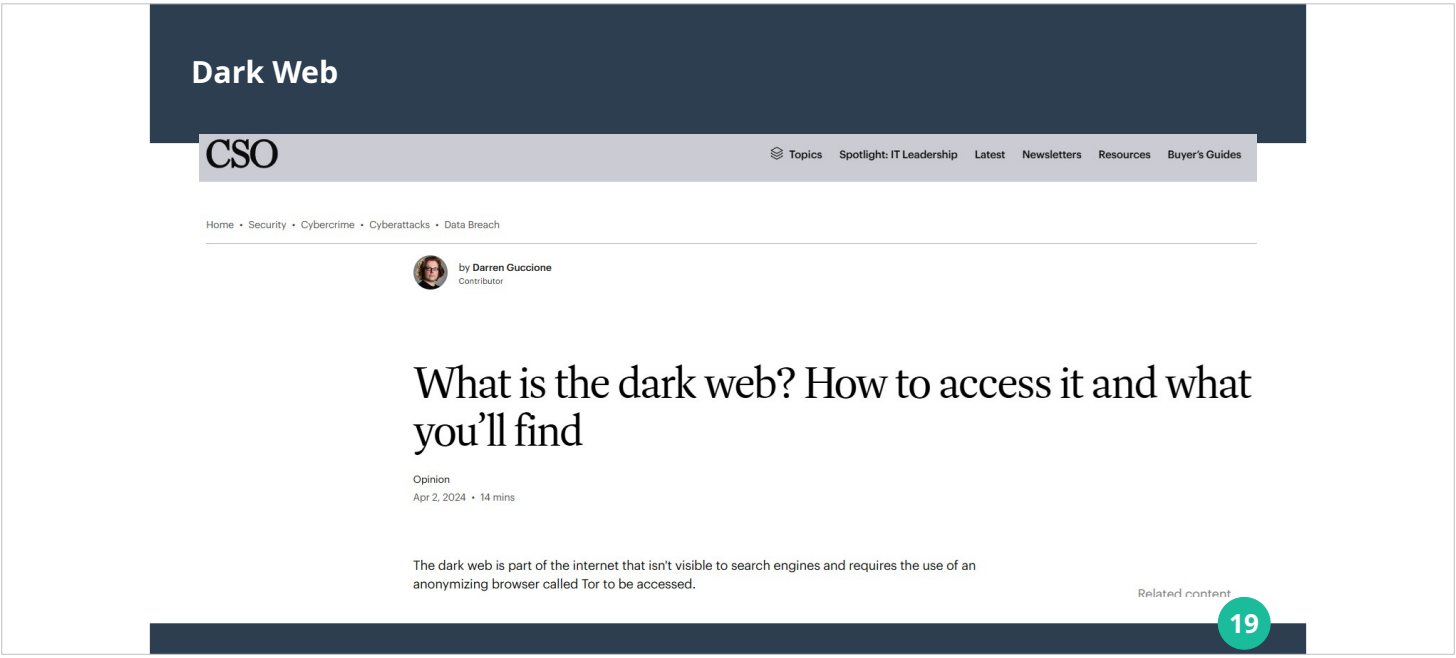
Then, we will venture into identity theft, what it is and how to prevent it.




The Dark Web is a collection of secret websites, marketplaces, photo and video databases, and lots of information and data, both legal and illegal, that's for sale.

Popular search engines like Google don't touch the Dark Web nor is it possible to simply pull up a website that's part of the Dark Web. One needs a special, private and anonymous browser called Tor to access the content here. It is difficult though not impossible to trace either the visitor or the website because Tor, unlike regular browsers, takes a round-about way to get to where it needs to go. We need to know about the Dark Web, but don't want to go anywhere near it. It is like the rough part of a tourist destination that we need to be aware of, so we don't end up there.

Scammers are able to buy their tools of the trade, like malware and spyware programs, on the Dark Web, which they then use to hack into accounts, steal data, and return to the Dark Web to sell it to other scammers. At some point in this chain of events, a scammer would have enough data to use it to actually cause us real harm, like commit identity theft or steal money.

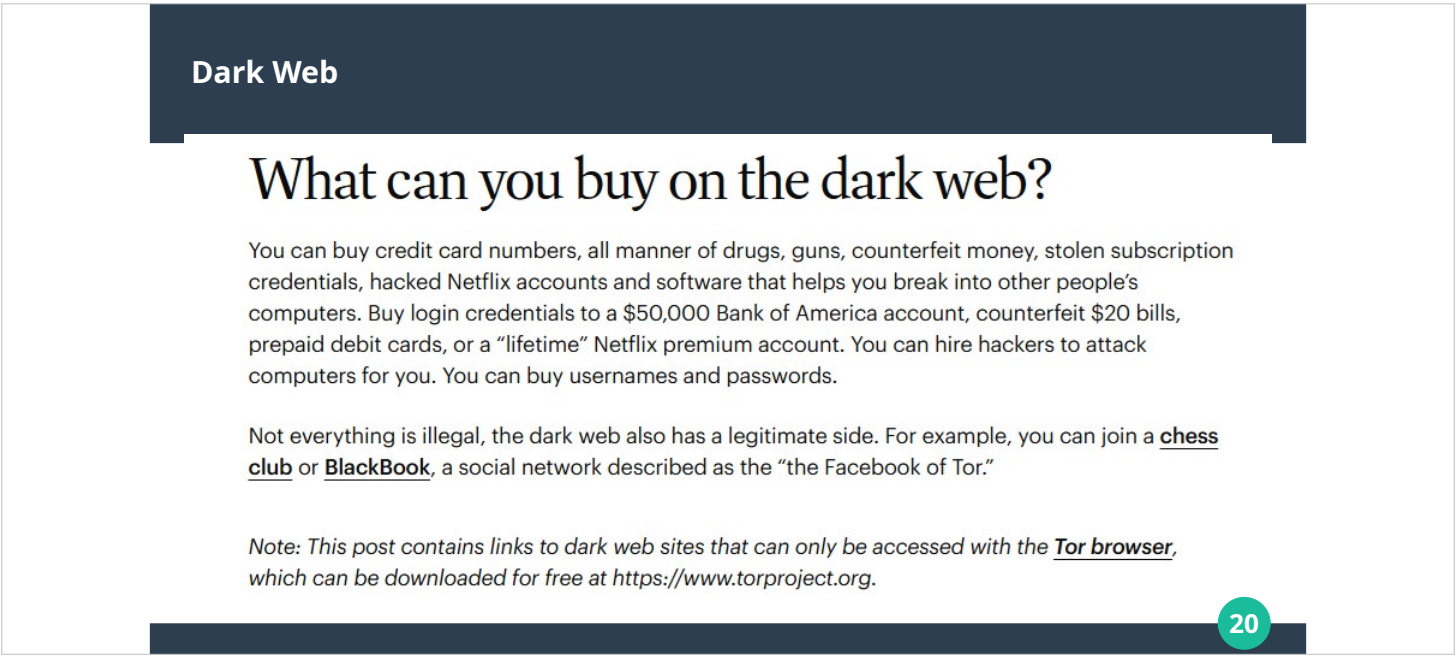



There are professionals in the cyber-security industry whose job it is to visit the Dark Web and keep tabs on the latest threats it poses to the world. They are like police detectives who might go undercover and visit the places where gang activity happens, so they can protect the community from all the ill-effects.

This is an article on the Dark Web, written by a security industry professional in a trade publication. If you're curious, there are many such articles and reports on the Internet. There are also some interesting videos on YouTube.

Big Tech companies like Google and Facebook spend millions of dollars on both human and automated methods to keep the more horrifying aspects of the Dark Web from spilling over into their search results and social feeds.

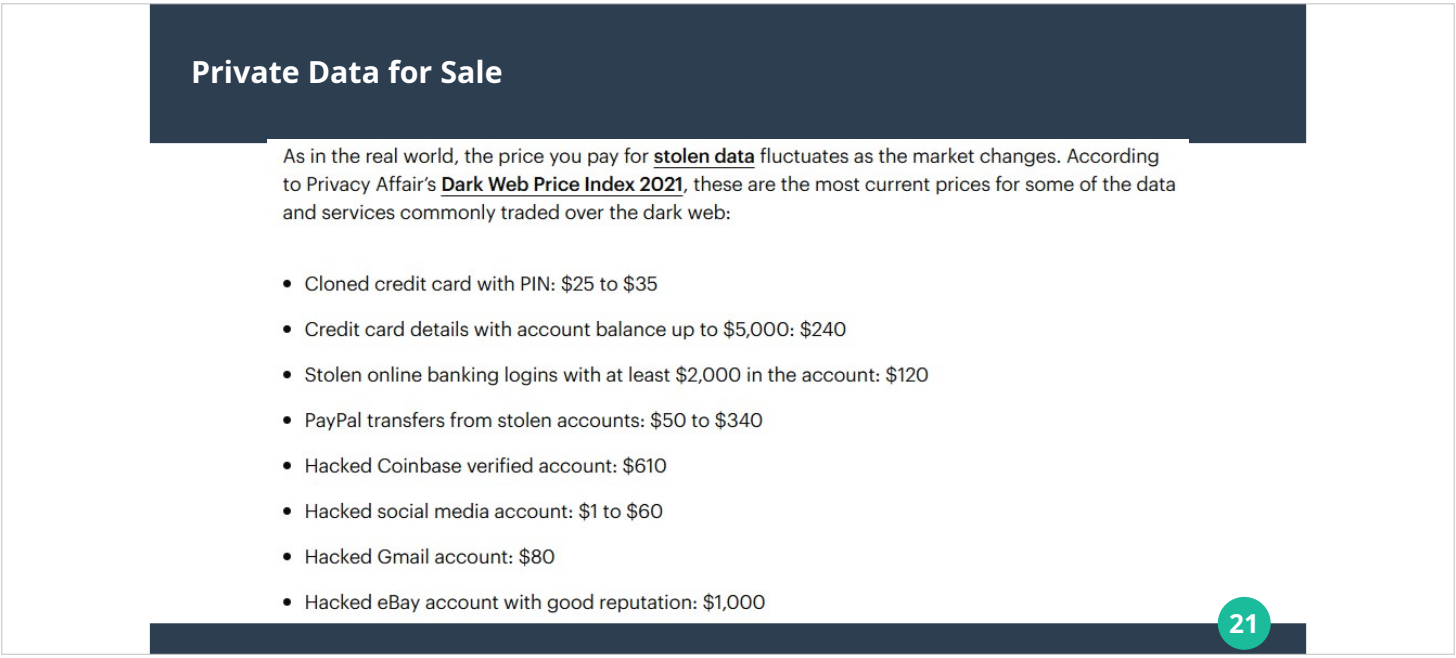
Unfortunately, no government or tech company can shut down the Dark Web. Law enforcement has successfully taken down specific websites and marketplaces that deal in illegal items, but as a whole, the Dark Web can't be taken down. The technology is out there and it will be used and innovated upon. The Dark Web can only be understood and its effects avoided.




Some of the things a scammer can buy on the Dark Web:

Stolen credit card numbers and pins, all manner of drugs - legal, prescription and illegal, guns, counterfeit money, stolen credentials like usernames and passwords, hacked Netflix accounts, computer programs that help with breaking into other people's computers, personal information like names, addresses, social security numbers, etc. A scammer can hire other scammers to do some of their dirty work for them. Scammers also invent new techniques and franchise them out to other scammers to expand their reach. It's a whole ecosystem.

The Dark Web is like a pirate ship. It's a miniature city, just as a cruise ship is a small floating city. Just as there are workers of all kinds on a cruise ship, from cooks to cleaners, medics, bartenders, mechanics, etc., there are entire communities and forums on the Dark Web where scammers with different skills hang out, chat and collaborate with each other on new schemes. Apparently, they have a social network called BlackBook and even a chess club!




Here are the going rates for some of the things a scammer can buy on the Dark Web:
A cloned credit card with PIN - $25 to $35
Credit card details with an account balance of up to $5,000 - $240
Stolen online banking login and password with at least $2,000 in the account - $120
Paypal transfers from stolen accounts - $50 to $340
Hacked Coinbase verified account for Bitcoin - $610
Hacked social media account – Up to $60
Hacked Gmail account - $80
Hacked eBay account with a good reputation - $1,000
Note that current, verified information fetches a higher price than old and possibly outdated information. Scammers are always looking to verify the information they get their hands on, which explains the high number of phishing attempts.


Knowing what we know about the Dark Web and all the danger that it poses to our safety on the Internet, how do we secure our assets online, like our bank accounts, email accounts, and subscription services?

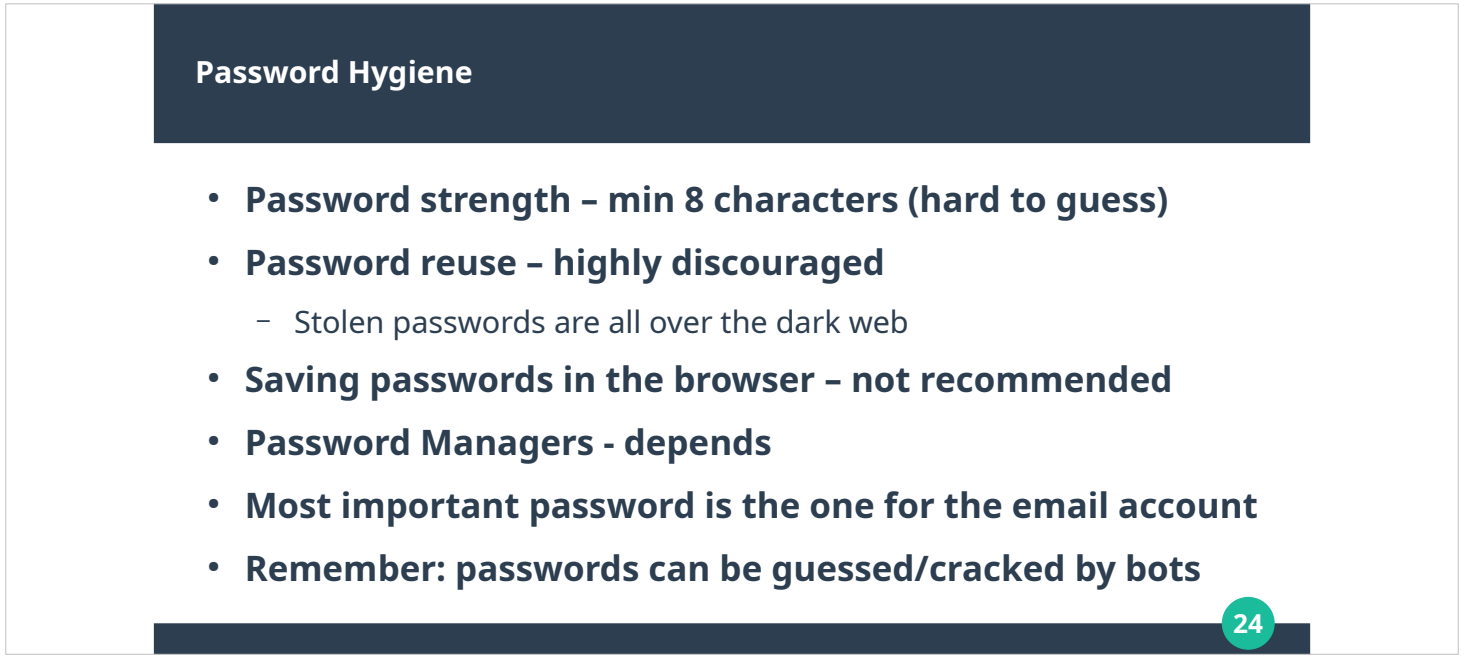
With good password hygiene. Let's talk about passwords.


Microsoft reported that their security department blocks over 600 million password attacks daily. That's over 7,000 attacks per second. These are attempts to hack into the services they provide to people like us, like Outlook and Hotmail email.

The majority of these attacks utilize password spraying, phishing and brute force techniques, often exploiting reused or weak credentials. If a scammer gets their hands on a thousand stolen passwords, one of the first things they do is to check which websites can be hacked into with those stolen passwords. This is because many people use the same password for multiple online accounts.

88% of basic web application attacks involve stolen credentials. A 2026 breached password report analyzed more than 6 billion passwords stolen by malware the previous year alone. Malware and spyware programs are installed on unsuspecting victims' computers which record passwords and send to the scammers.

Password attacks or identity attacks surged 32% in the first half of 2025.




Here are some good practices to maintain with passwords, also called password hygiene.

A minimum of 8 characters, preferably 10 or more, with random letters of both upper and lower cases, numbers and special characters. Passwords with words from the dictionary or people's or location names are easily cracked by software.

A single unique password for each online account or service. Imagine a hacker stealing your Netflix password and trying it on your bank account and finding out it works! It's certainly more work to make up new passwords every time but it's worth it.

It's convenient to save a password in the web browser and have it auto-fill it when we visit a website's login page but it's safer to not store passwords on the computer at all, but instead, write them down in a book and keep them completely offline.

It's the same with online password managers that promise convenience. The promise is: you need to remember just one password and it unlocks all the others. But it's like keeping all your eggs in one basket.

The most important passwords are those that let you in to your financial accounts and your email accounts. This is because, if you forget your bank password, they will send you an email to reset it. So a compromised email account is essentially the same thing as a compromised bank account.


LastPass is a password manager that promised convenience to its users. Their promise, going by the name, is: the last password you'll ever need to remember! Just remember the password to your LastPass account and you'll have access to the passwords to all your other accounts – so went the promise.

There are many password managers on the market that offer this convenience. Some of them will even create a new, strong password when you sign up for a new online service and enter it for you automatically when you visit the service in the future. No need to keep track of a dozen or more passwords for all your accounts.

It is indeed a real problem that we, modern Internet users, have when we need to create and keep track of so many passwords. But there is no good solution for this problem. It's best to write them all down or, at the very least, avoid storing them on any and all Internet-connected electronic devices.

LastPass got hacked and 1.6 million users were exposed in the data breach. It's a terrible security failure when all your passwords are in one place and they are suddenly up for sale on the Dark Web.


These days, passwords alone, as important as they are, are not enough to secure our online accounts. With a password alone, it's virtually impossible for any bank or a company like Amazon or Google to completely prevent password attacks and unauthorized access by hackers and scammers. The industry needed another way to make sure the person attempting to login into an account is indeed who they say they are. So they invented a new mechanism to secure accounts in addition to passwords.

This is called 2 Factor Authentication, or 2FA. It's also sometimes called MFA, which is Multi Factor Authentication. For our purposes, 2FA and MFA are the same.

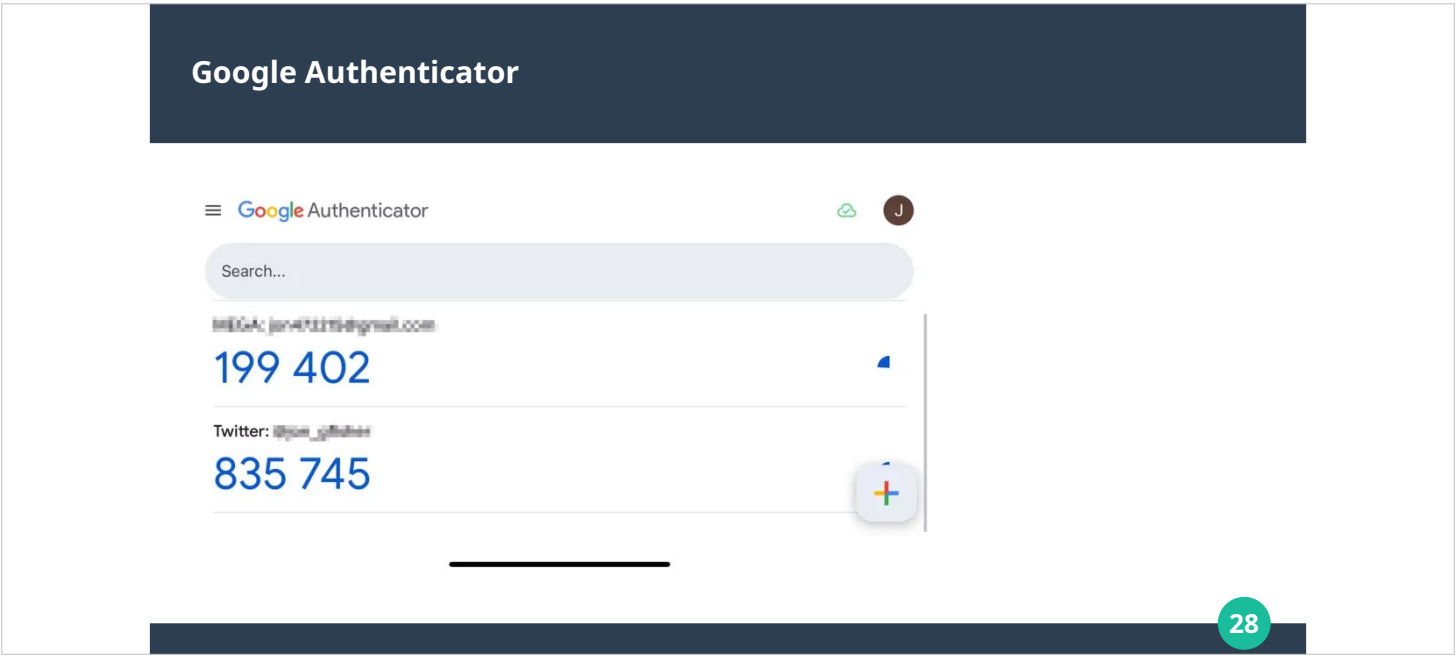
You probably already use it without realizing that it's referred to by this terminology. If you try to login into your bank account and you are asked for a 6-digit number that's been sent to your phone, that's 2FA in action. Most companies and government agencies like the IRS and USPS offer 2FA to their customers to better secure their accounts. But only some require its use while the rest leave it optional and allow the customer to choose if they want to make use of the facility or not.

While 2FA helps an organization be more certain that it is indeed their customer who is trying to login, it helps us, the customer, even more by preventing scammers from getting into our accounts. So if a company or organization we have an account with offers 2FA, it is highly recommended, from a security standpoint, to opt in and set it up.


The idea behind 2 Factor Authentication is that the customer needs to provide 2 pieces of information to prove that they are legitimate. One is “something we know” and the other is “something we have”.

The first factor is the password and this is something we are supposed to know. Even if we write it down, this is still in the category of “something we know”. The second factor is typically a device that we own and this satisfies the requirement of “something we have”. So when a bank sends us a 6-digit code by text message, they are actually making sure we have our phone with us, because the phone number they sent it to is linked to our phone. A scammer might get their hands on our password, but they don’t have what we have – our phone – and so cannot get that 6-digit code to use as the second factor.

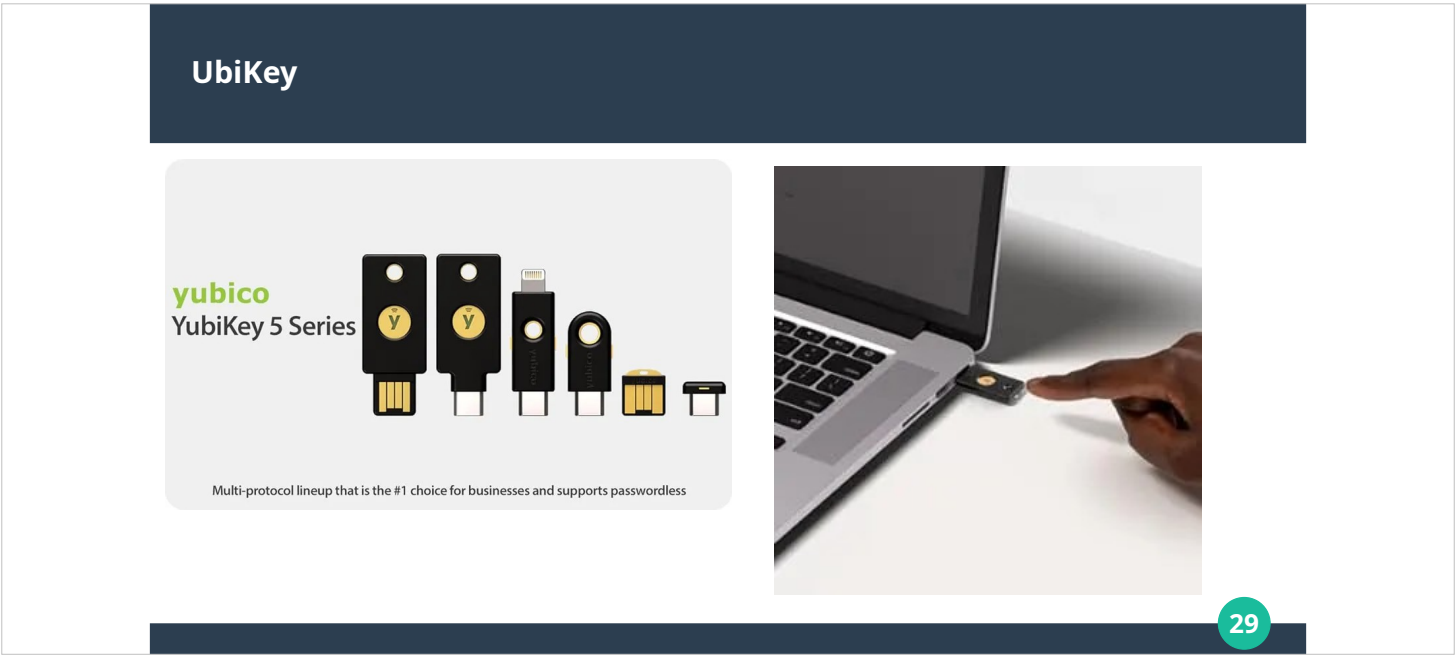
So we see how using 2FA helps us better secure our online accounts. In addition to our smartphone, there are other things that can be used as a second factor, like our fingerprint. We still use our phone to scan our fingerprint, but it’s distinct from our phone number when used as the second factor. There are two other forms of second factor that we will talk about next but the phone, verified by a text message sent to its phone number, is by far the most common 2nd factor in use today.




Another type of second factor is what's called an Authenticator App. Google Authenticator is one such authenticator app, but there are others like Microsoft Authenticator and Proton Authenticator. These are apps you install on the phone, just like any other app, from the Google Play Store or the Apple App Store.

An Authenticator app is tied to our phone, which is in turn tied to our Google or Apple account. So, this form of second factor also makes sure that we have our phone with us and satisfies the requirement of "something we have", even though our phone number is not involved. So the difference is, instead of entering a 6-digit code we receive by text message sent to our phone number, we enter a 6-digit code that the app provides. This code changes frequently (like, every minute) and is known only to us and the company we're logging in to.

To use an Authenticator app as our second factor, we have to choose this option when we set up our 2FA in our bank or other online account. Not all banks and companies offer this option, but if they do, it's recommended to choose this over text message.

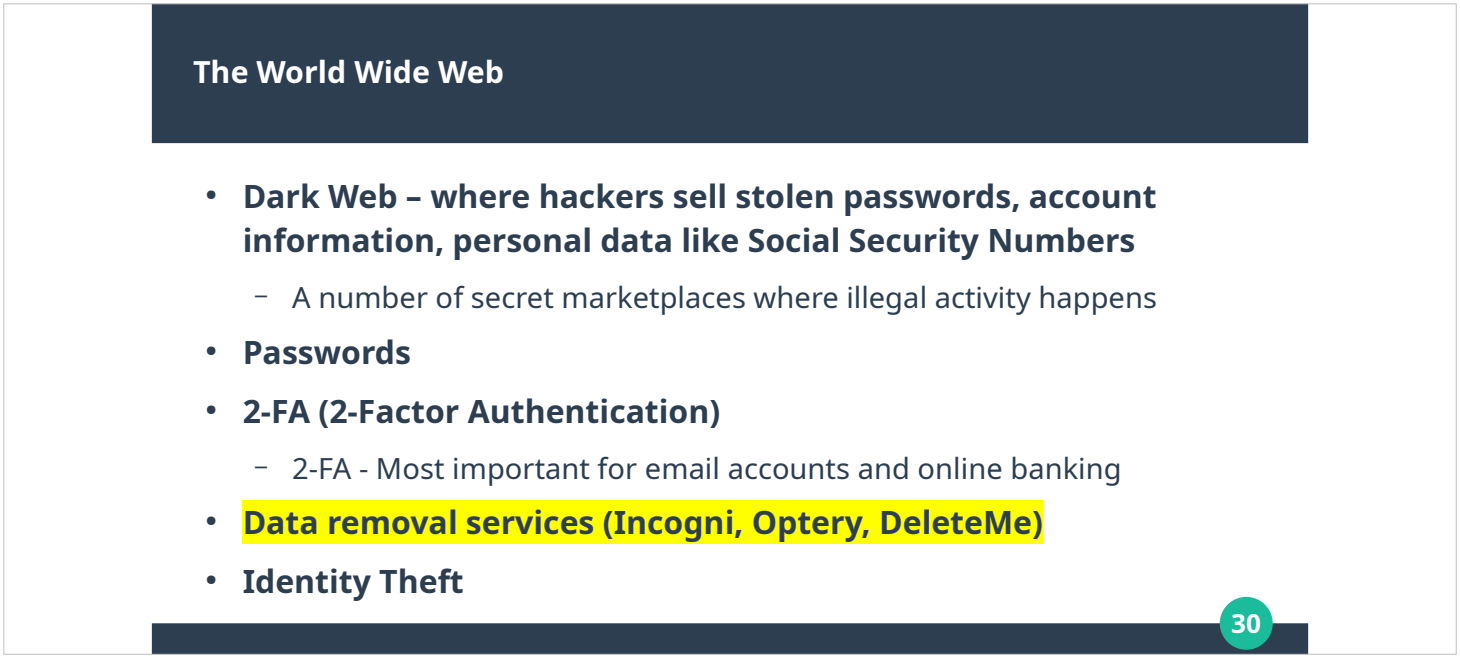



We've seen 2 types of second factors – the text message sent to our phone number and the Authenticator app both of which are tied to our smartphone. The phone is the "something we have".

Another type of second factor that we can use, if our bank or another company offers it, is the physical key. This type has nothing to do with our phone, and is a pure form of "something we have", because it's sole purpose is to be a second factor.

The YubiKey is one of the popular ones on the market. They come in different shapes and run anywhere from $25 to $100 depending on features, but basically, we plug them into the USB port of our computer or laptop, and it fills in the code automatically when needed. Some of them have an additional safeguard, like a fingerprint reader, so we can be sure that it can't be used even if it's stolen.

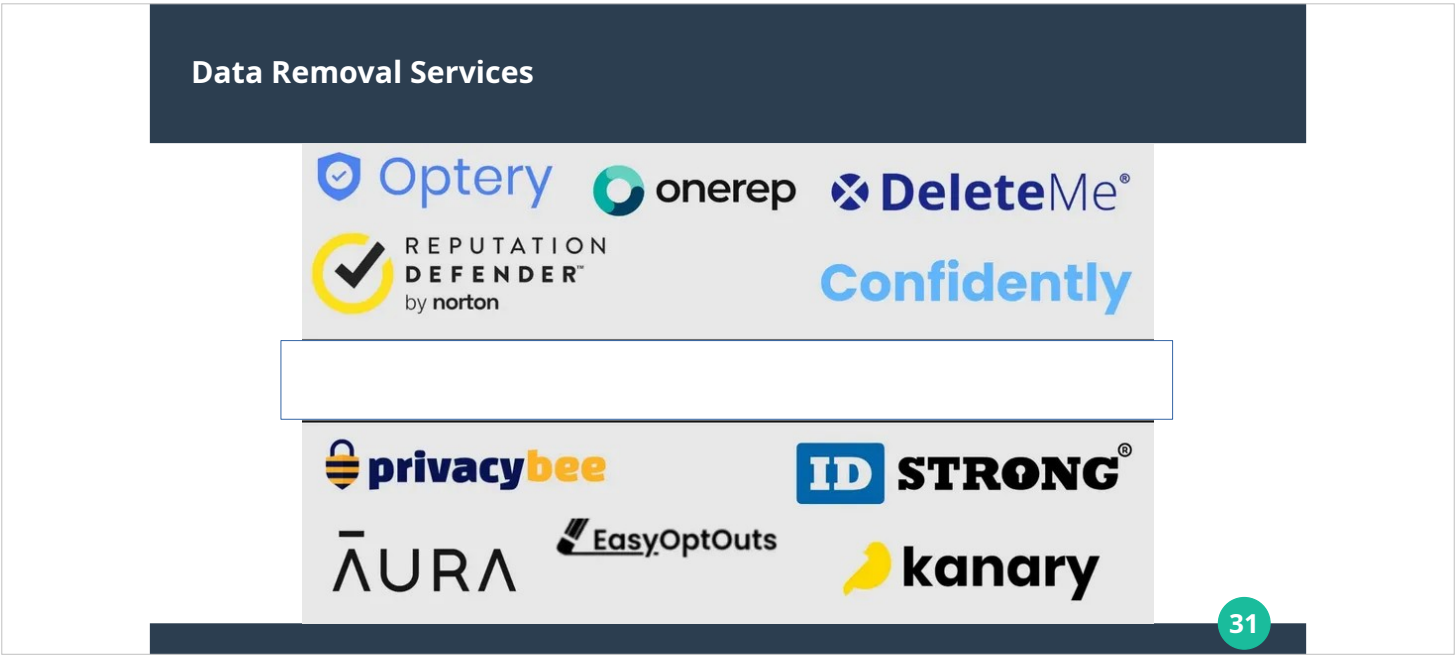
Physical keys are a superior option compared to either of the phone-based options. Although not very common yet outside corporate environments, their use is growing slowly as more banks and companies begin to offer them as an option.




Over the last 25 years, as Internet use has grown exponentially, so has the number of data breaches. A data breach is a successful attempt at hacking into a company's computer systems and databases to steal information. Hackers gain access to this information at which point they may decide to sell it on the Dark Web or simply expose it online. Several large companies have been breached in the last two decades – Facebook, Instagram, Yahoo, Marriott International, Equifax, Ticketmaster, Sony Playstation, Qantas Airlines, Aflac, the list goes on.

The personal information of 500 million guests was stolen in the Marriott breach. 147 million Americans had their private personal information exposed in the Equifax breach. Yahoo – all 3 billion user accounts!

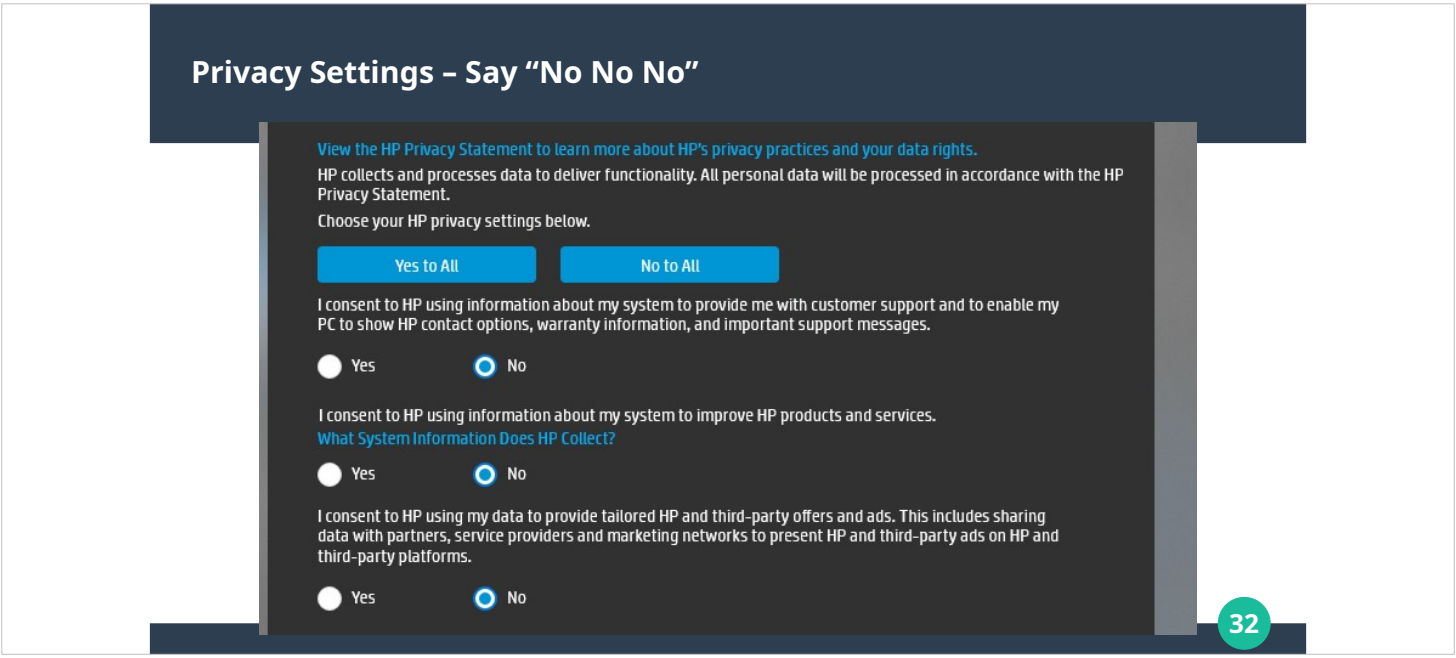
Our information is out there on the Internet. Several companies buy and sell our information for advertising and other purposes. Is there anything we can do about it?




There's no good answer to that question. The nature of the Internet is such that once something is out there, it is difficult to erase it. Electronic copies of our data are stored in dozens or even hundreds of locations.

There is an entire industry dedicated to helping us remove our personal information from the Internet. They fight a difficult battle because they cannot force a website that's dealing in our data to delete it. They can only make lawful requests and it is up to the company to abide by the law. In practice, this means that although many sites remove our data upon request, because they continually add new data to their systems, it is likely that our information will reappear on their site in the future. Not to mention the hundreds of new websites that come into existence every year. It's like whack-a-mole. Delete information on one website and it pops up on a new one.

This isn't exactly bad news for the data removal service industry, because they get to charge us monthly fees to keep at it forever. It is up to you to decide if it's worth spending money every month to chase a moving goalpost. If you're curious, you might want to sign up for a trial with one of the companies shown here, and see what they do for you.




So how does so much data about us get out there in the first place? Much of it is information that companies require us to fill in when we sign up for their services. But some of it is optional and some, they just take from us without our knowledge. The less we allow them to take, the better for us.

This is the link between online privacy and cyber safety that comes up throughout this series of presentations. The more we get into the privacy settings in our computers, smartphones, apps, and online accounts, and the more we opt out of the data collection practices that companies have, the higher our privacy and hence also security.

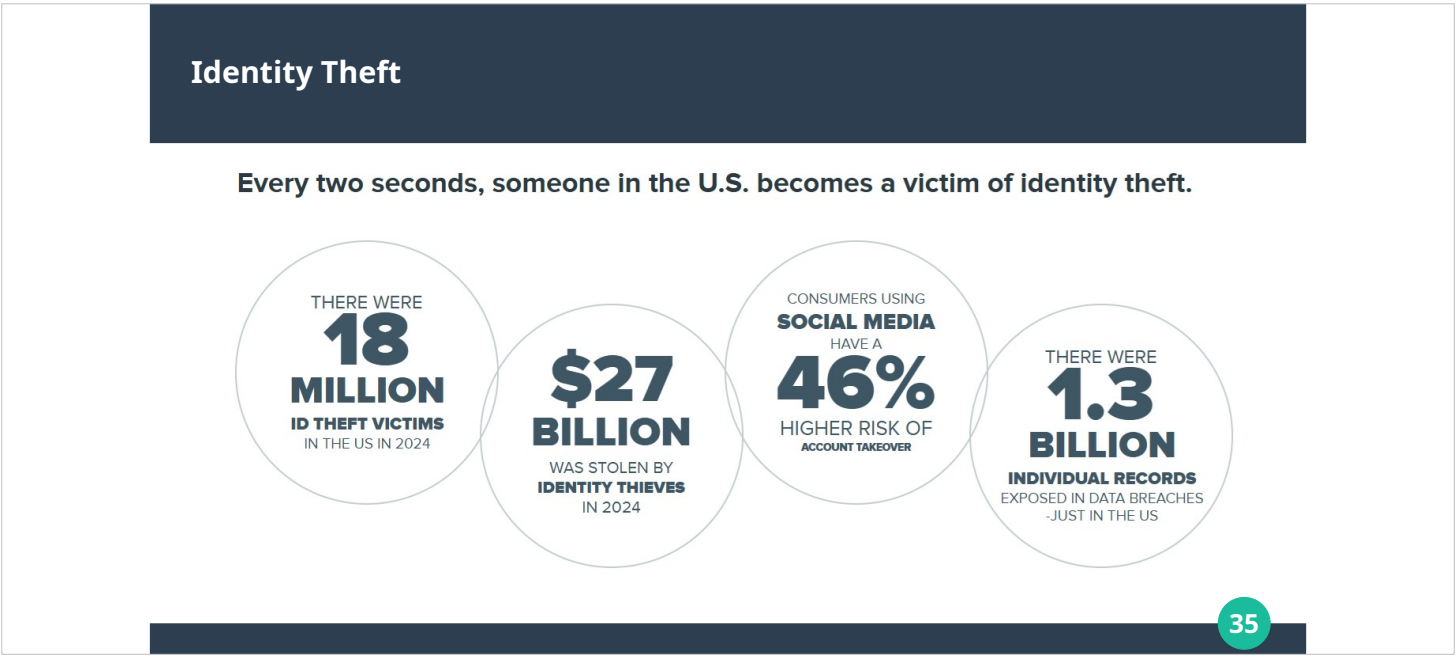
This is a screenshot of the privacy settings presented by a HP printer software program. The best practice is for us to click on “No to All” which prevents HP from collecting our personal information that they would otherwise sell to third party marketing and advertising partners. The less we share with HP and its partners, the less we put at risk in case they suffer a data breach.


The higher our exposure, the higher the risk of becoming a victim of identity theft. Identity theft is one of the more insidious scams out there, partly because, we generally have no idea it's happening to us until it's too late. At that point, the victim is left with stitching back their life together. This involves hiring attorneys and convincing several different banks and companies that we're the real so and so, and not the scammer who impersonated us.

Identity theft is a deliberate, coordinated, well-thought-out plan by a cyber-criminal or gang to impersonate a victim in multiple ways, using a number of different pieces of information they know about the victim, over a period of weeks, months or even years. It's a super-charged form of impersonation where the scammer becomes the victim, takes on their name, contact information, mailing address and more.

It's a growing menace and is hard to detect unless we proactively monitor for it. It is, however, possible to significantly reduce the chances of being victimized by following certain simple and effective steps which we will go over soon.

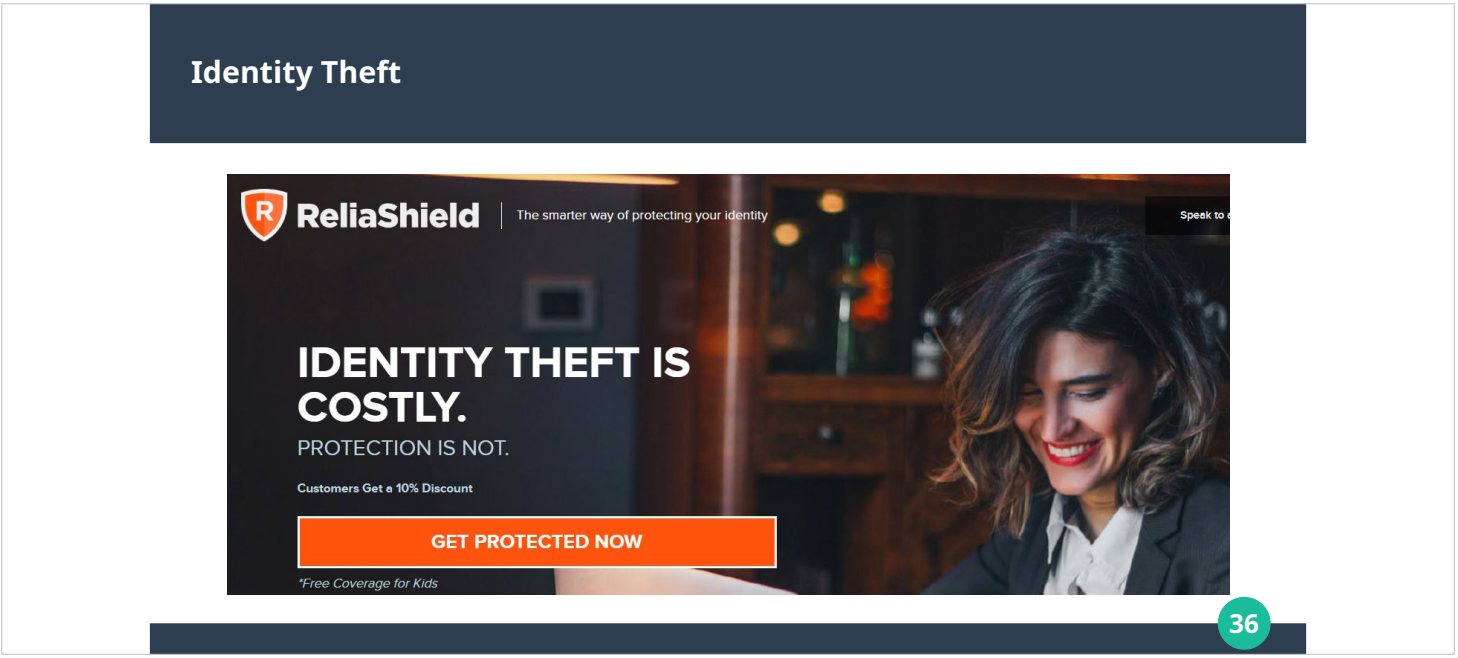

These are some of the things an identity thief can do:
They can steal money from your bank and investment accounts.
They can take out loans and mortgages in your name.
They can file taxes in your name and obtain refunds directly from the IRS.
They can apply for and obtain credit cards in your name and run up the balance.
They can ruin your good credit history.
They can obtain phones and cell phone plans in your name and use them to commit crimes.
They can even commit felonies and other major crimes using your identity.




Every two seconds, someone in the US becomes a victim of identity theft.
In 2024 alone, there were 18 million victims of identity theft.
In that year, $27 billion was stolen by identity thieves.
People using social media like Facebook have a 46% higher risk of having their accounts taken over and used for identity theft.

Identity theft is made possible because a lot of information about us is exposed online. This information comes from billions of individual records that are leaked from corporate databases and systems in data breaches.

The victim of an identity theft suffers due to no fault of theirs. It is the company or bank that they have a business relationship with that happens to fail at being a good steward of the data that it's entrusted to take care of.

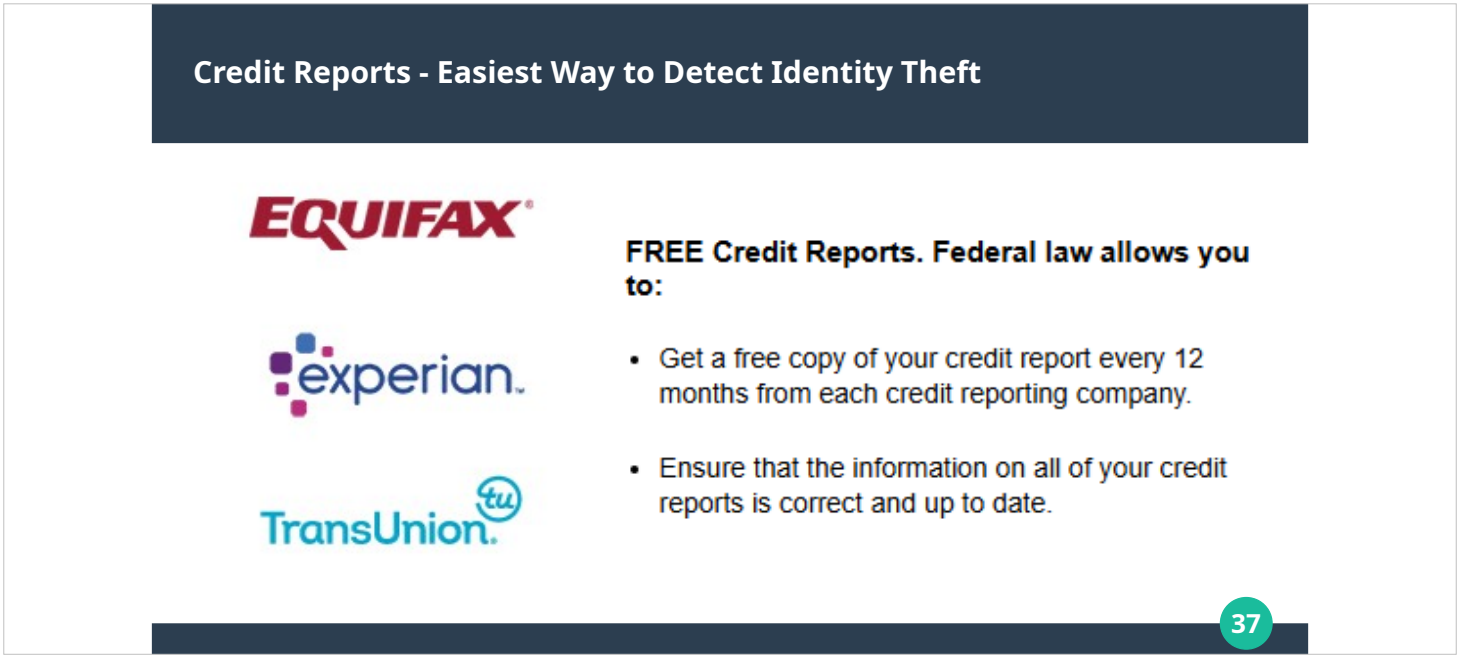



Identity theft has become such a big problem that there are companies offering insurance plans to help us recover from its after-effects. It is a very time-consuming, expensive and stressful process stitching back our identity together after it's been ruined.

The big insurance companies like GEICO, State Farm, All State, as well as specialty providers like the one shown here, called ReliaShield, all offer identity theft insurance that includes monetary compensation and legal assistance.

Note that these plans provide limited protection, specifically targeted at the losses from an identity theft scam. They don't cover all the other types of cyber scams where the victim has played an active, if unwitting, role. For example, if a scammer gets a victim to reveal their login credentials through a phishing attack or obtains a 6-digit one-time-passcode or OTP directly from the victim over the phone, and subsequently steals money from their bank account, these plans don't cover the losses. In many cases, the bank also refuses to cover such a loss because the victim was not supposed to give their OTP to anyone.

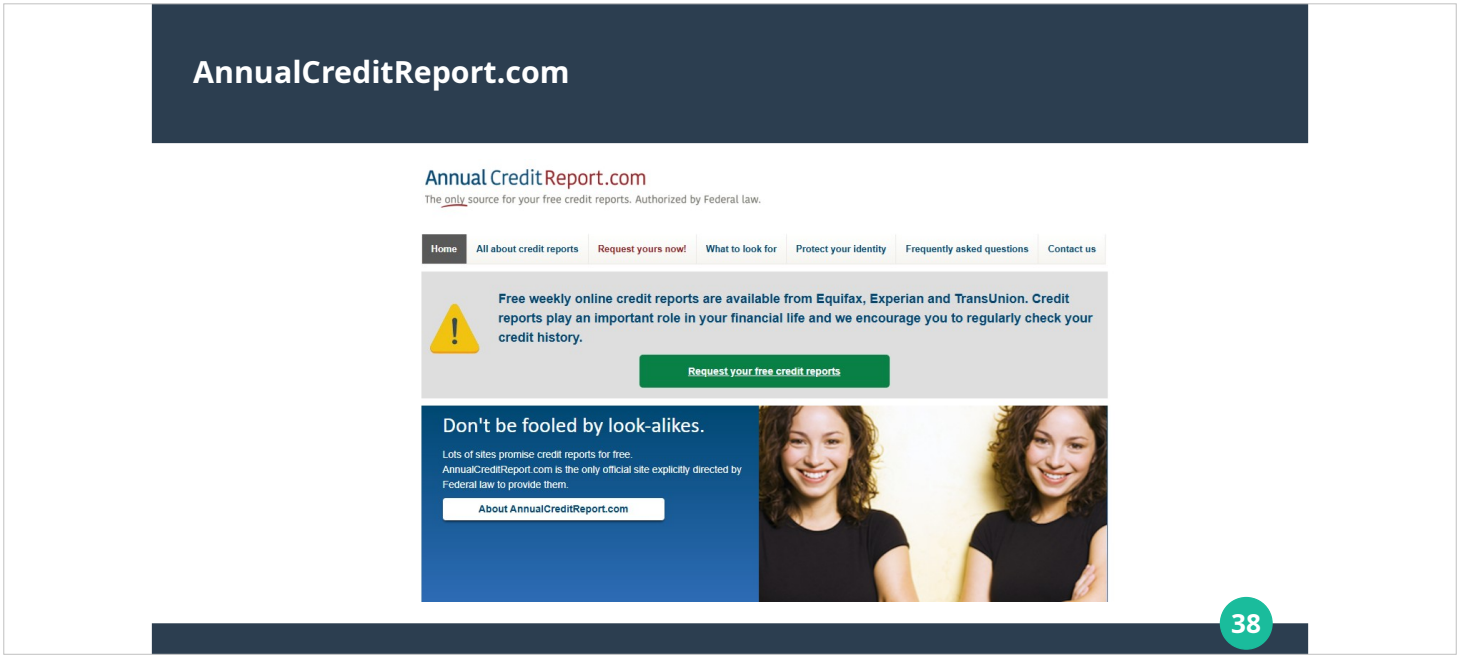
We cover many different types of cyber scams in the next presentation, presentation 102, so be sure to check it out.




One of the easiest and most effective ways to detect an ongoing identity theft scam in our name is to monitor our credit reports.

You may have heard of these three companies – Equifax, Experian and TransUnion. They are called consumer reporting agencies. They are also called credit reporting agencies or credit bureaus, because they maintain credit history files on all Americans. These files are referred to by other organizations in their course of doing business. For example, banks use them when they issue credit cards, cell phone companies look them up before enrolling a customer on a plan, and leasing offices refer to them before renting out an apartment. They're an integral part of American commerce and economy.

By law, these three credit reporting agencies are required to provide everyone they have a file on, which is you, me and everyone else, a copy of their file once an year, free of cost. This file, also called a credit report, shows many details of our financial history and should be treated as confidential. It also contains non-financial, historical information such as the addresses we lived at, names we used, phone numbers we had, companies we worked for and any public records. More importantly, it shows all the lines of credit (loans, mortgages, auto loans, credit card accounts, etc.), those that were open in the past and those that are currently open in our name.




It's this information that we monitor periodically to make sure that all the accounts that the report says are open in our name are indeed ones we know of and recognize, ones that we opened ourselves. If anyone else has been using our name and social security number to open a line of credit in our name, for example, it would show up in the report and become a reason for further investigation.

To abide by the law Congress passed, requiring them to grant a free credit report to every person once an year, the three credit bureaus have teamed up and created a website called AnnualCreditReport.com. This is the official website where one can request a free credit report from one or more of these bureaus.

At this point, it shouldn't surprise us that there are several fake websites some of which look like the official one and have similar names. These show up in search results and scammers see them as easy ways to collect people's social security numbers, because a social security number is required to pull a credit report from the official website. So, we see a big warning on AnnualCreditReport.com about look-alike fake sites that pretend to be the official one.

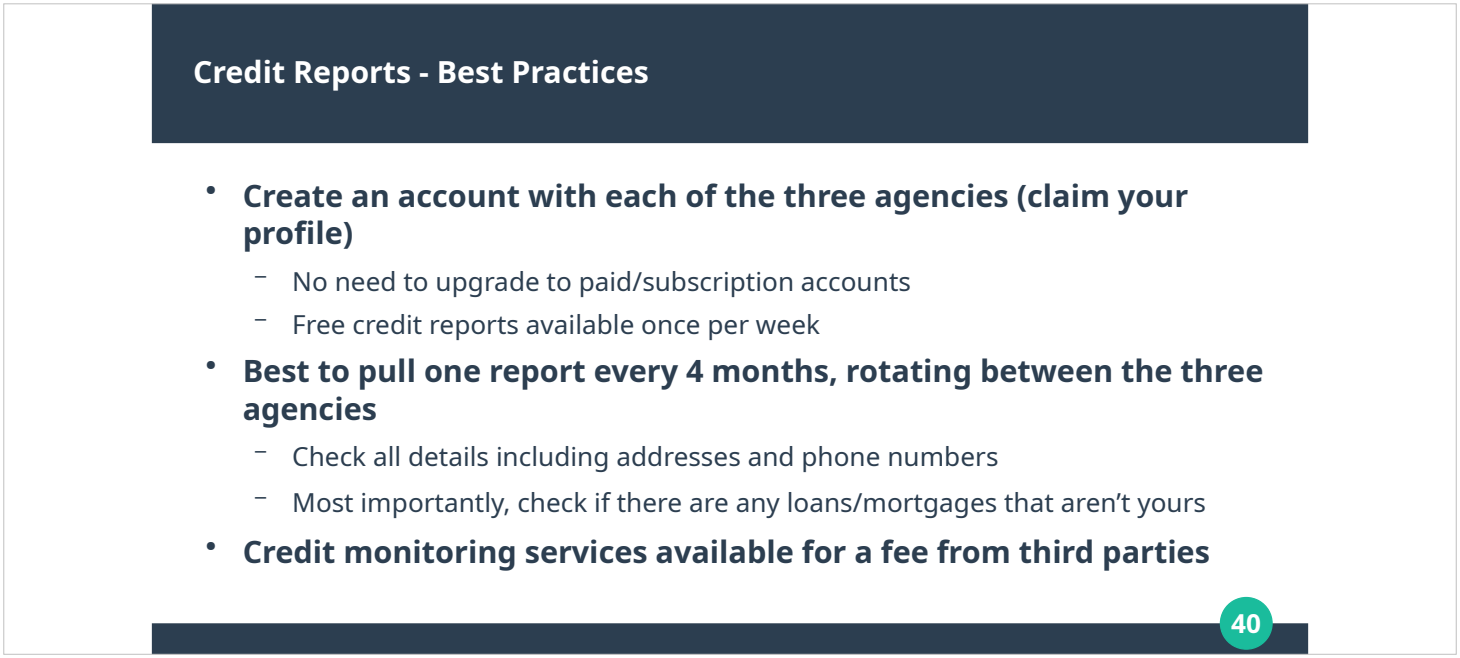
It's recommended to write down the name of the official website or bookmark it in the

## Legal Experts' Recommendation


39

A law firm that specializes in financial matters has this article on their website. It recommends checking AnnualCreditReport.com on a routine basis.

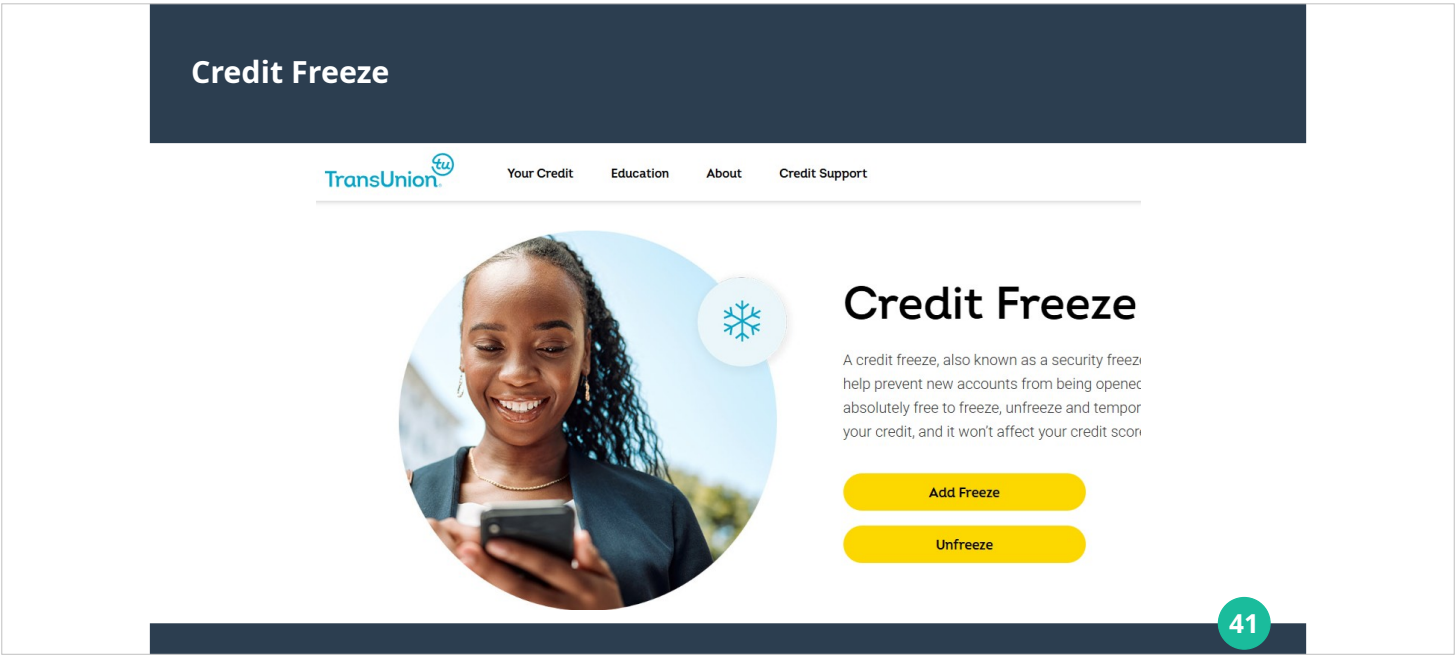
Several government agencies like the CFPB (Consumer Financial Protection Bureau) and the FTC (Federal Trade Commission) have articles and advisories on their websites discussing how you can get your free credit report from AnnualCreditReport.com




Many experts and financial advisors recommend obtaining one report every 4 months, rotating between the three agencies. This way, we pull only one report per agency every year, and that report is free of cost.

Thoroughly check the report for any new loans, credit cards, addresses and phone numbers that are not yours.

It is also advised to create an account directly with each of the three credit reporting agencies. They already have a file on us. Why not claim it? This not only prevents a scammer from creating an account in our name and claiming our file as theirs, but also unlocks free weekly credit reports, should we need to check them outside the routine. There's no need to upgrade to a paid subscription or set up automatic monitoring which are things they want you to do when you create a new account. These are fee-based services which are also available from third parties like banks.

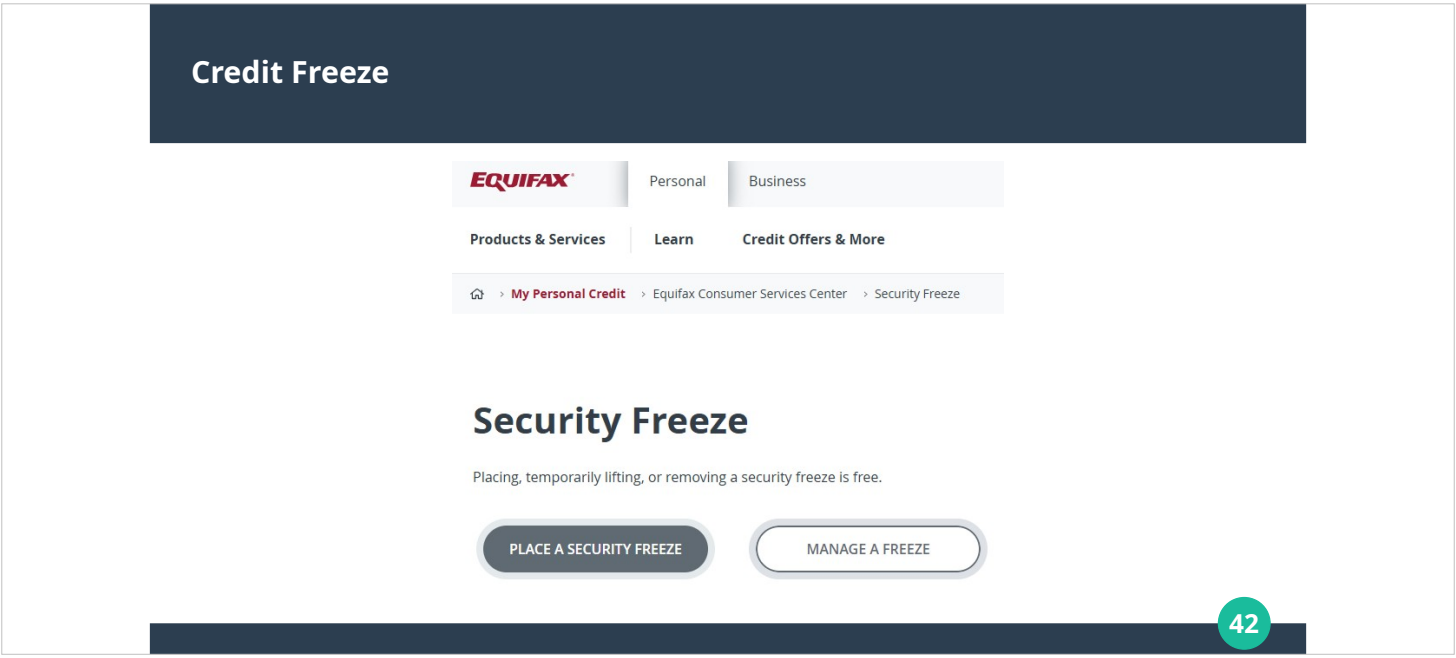



Another recommendation from financial and legal experts that significantly helps prevent identity theft is to place a freeze on our credit reports.

With a credit freeze in place, no one can obtain a loan using our name, because the institution that's preparing to give out a loan would need to assess our credit worthiness but would fail to obtain our credit report. The credit bureau would deny access to our credit report when requested by the institution.

Placing a freeze on our credit report does add some inconvenience when we ourselves need to apply for a loan, open a bank account, or rent an apartment, because we would first need to unfreeze our report, so it can be accessed by the institution that we're doing business with. But it's worth it.

Here's a screenshot of the webpage where one can request a credit freeze at TransUnion, one of the three agencies or bureaus.

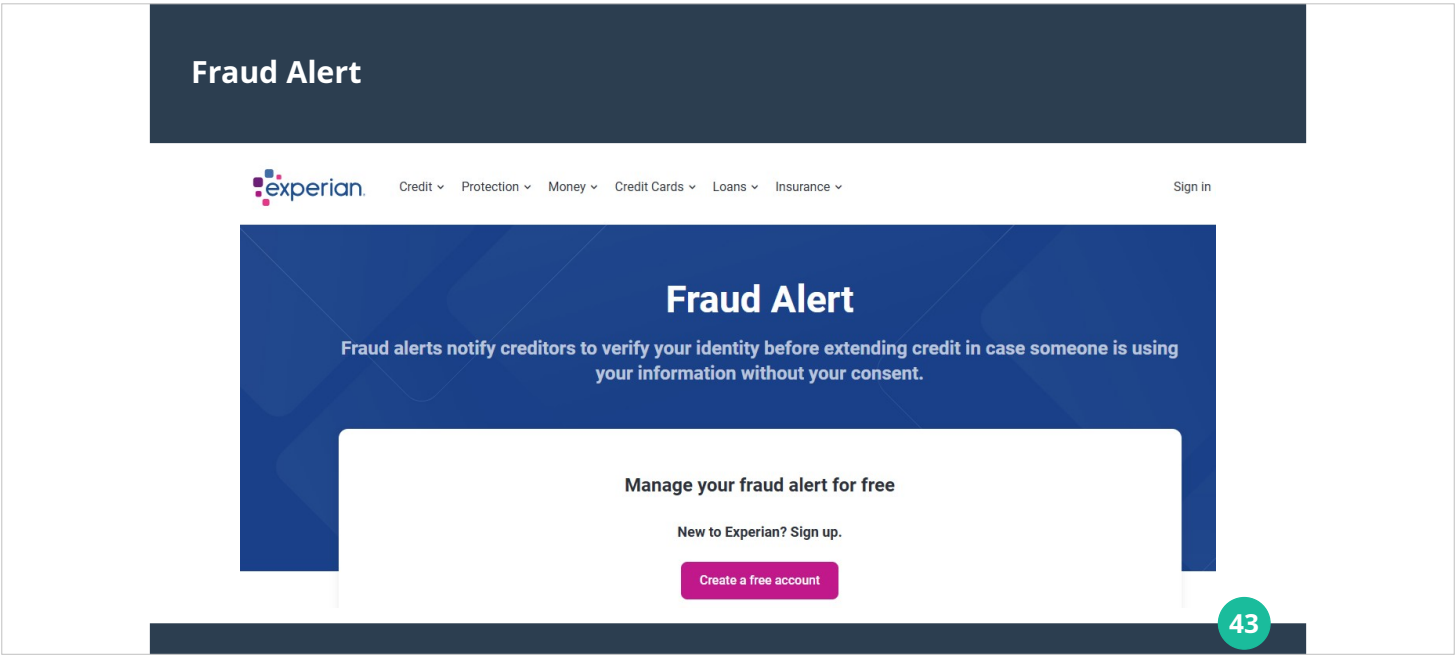



And this is at Equifax.

Note that they use slightly different terminology. Equifax calls it a Security Freeze. But it's the same as a Credit Freeze.

Because we don't know exactly which of the three agencies our bank or the apartment leasing office pulls a credit report from, it is necessary to place a freeze with all three of them.

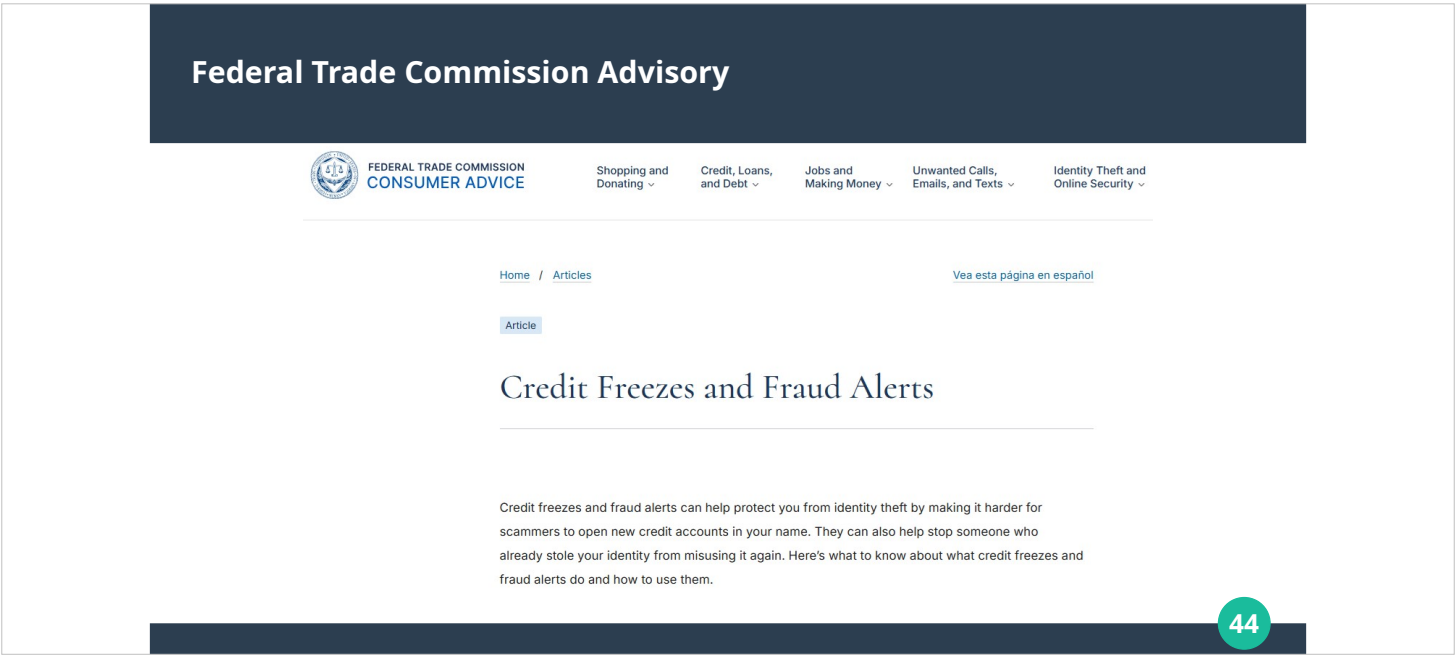
Again, the three agencies are TransUnion, Equifax and Experian.




There are times when we suspect that we're at a heightened risk from identity theft. Perhaps, we're already a victim of another type of cyber scam, or someone stole our wallet with our social security number and other details inside.

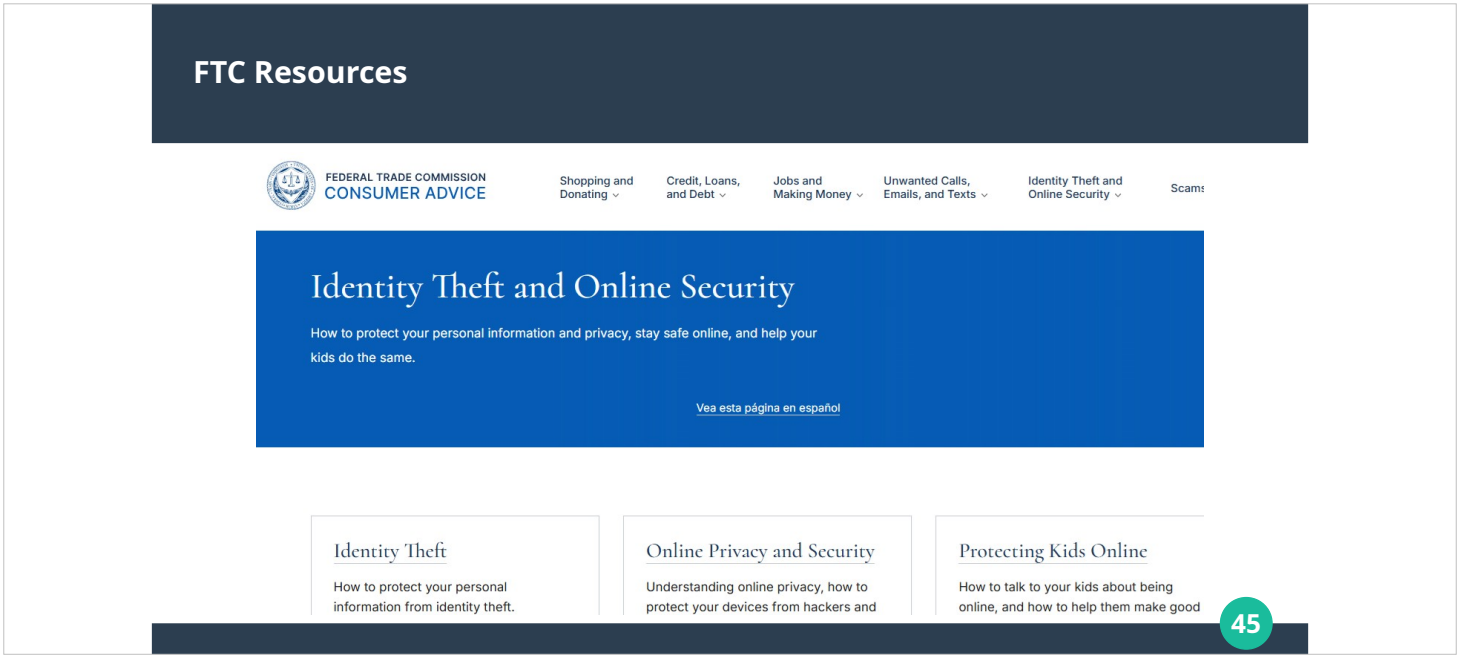
In such situations, we can place a Fraud Alert on our file at each of the three agencies. This is different from a Credit Freeze. A Fraud Alert lets the institution looking at our credit report in order to assess our credit worthiness, know that we've placed an alert, and that they should be extra careful and more vigilant before issuing a loan in our name due to our concerns about potential fraud. It stays on our file for one year after which it expires.

A Credit Freeze, on the other hand, stays active as long as we leave it on. When we need to unfreeze it, we request a 24-hour unfreeze after which it goes back to being fully active.

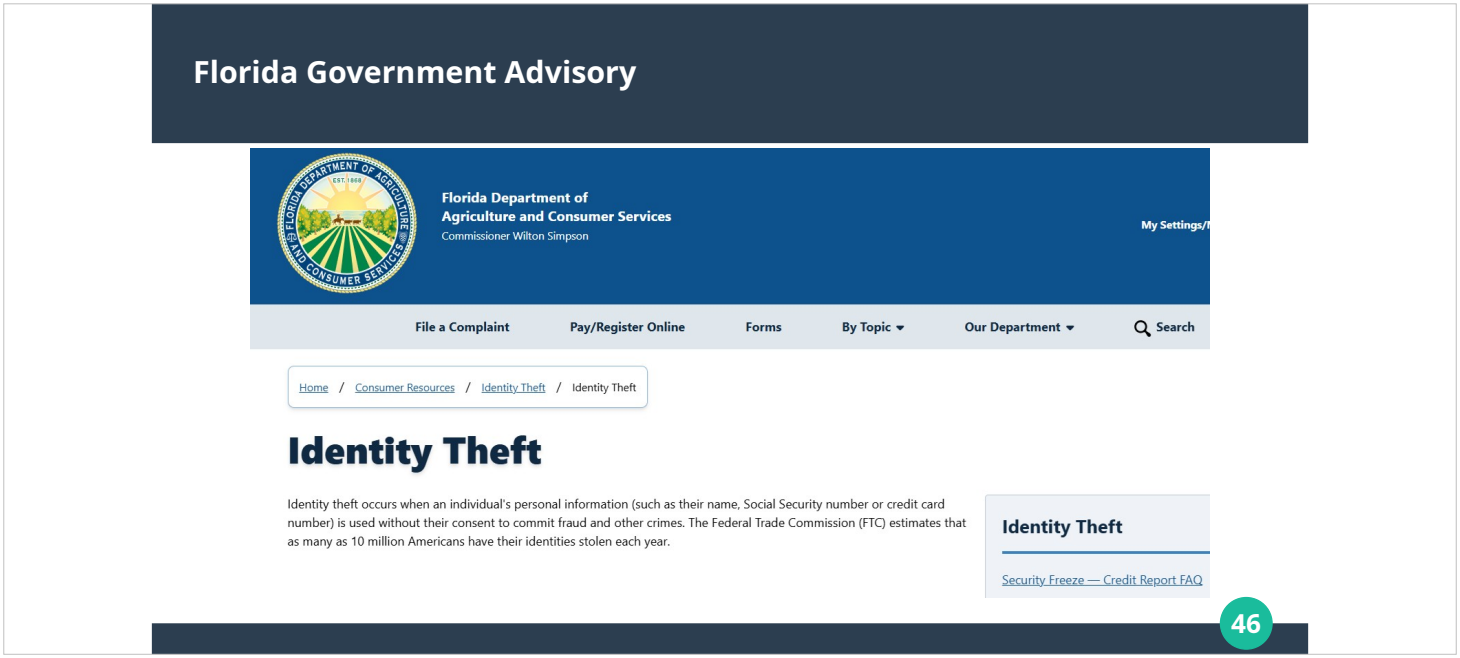



This is an article on Credit Freezes and Fraud Alerts on the website of the Federal Trade Commission (FTC)

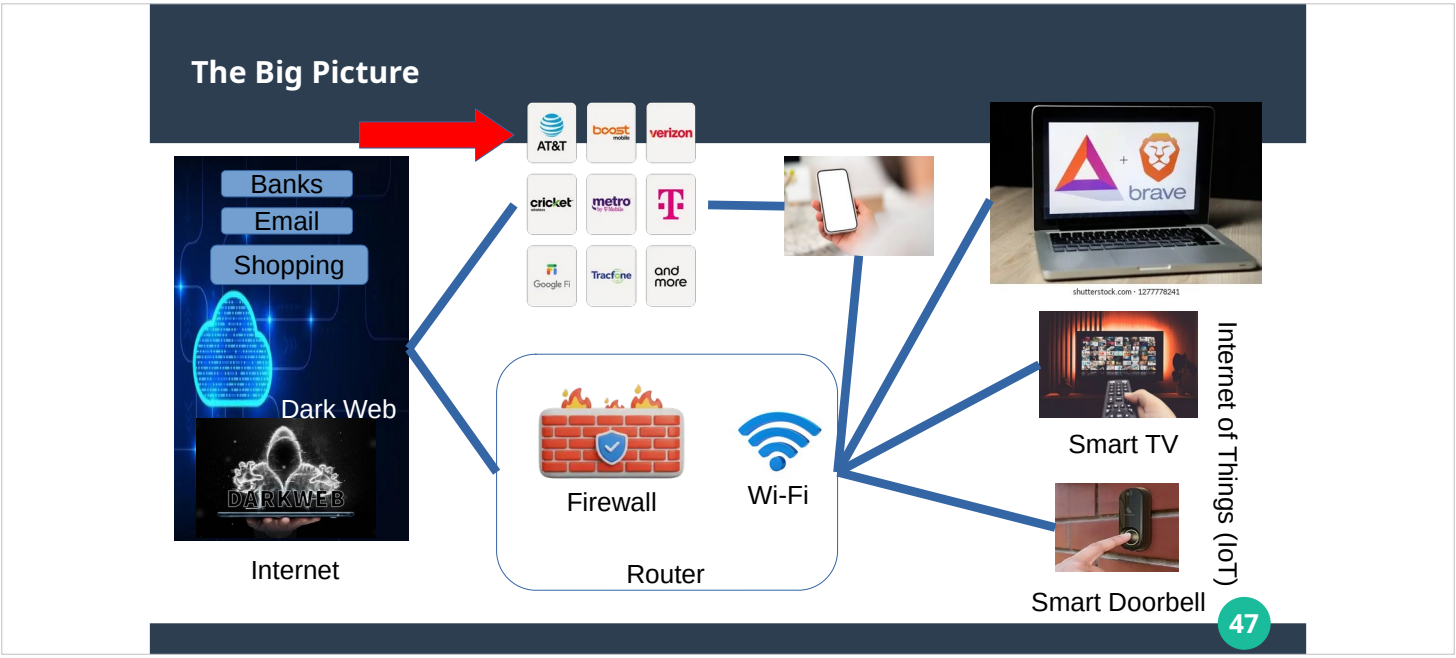
These are both very useful tools that the government and the credit reporting agencies provide all Americans and it is in our best interest to take some time and make use of them. They greatly diminish the chances of identity theft happening to us.




The FTC has a number of articles on their website offering valuable advice on protecting ourselves and our families from identity theft and other scams, while staying safe online.



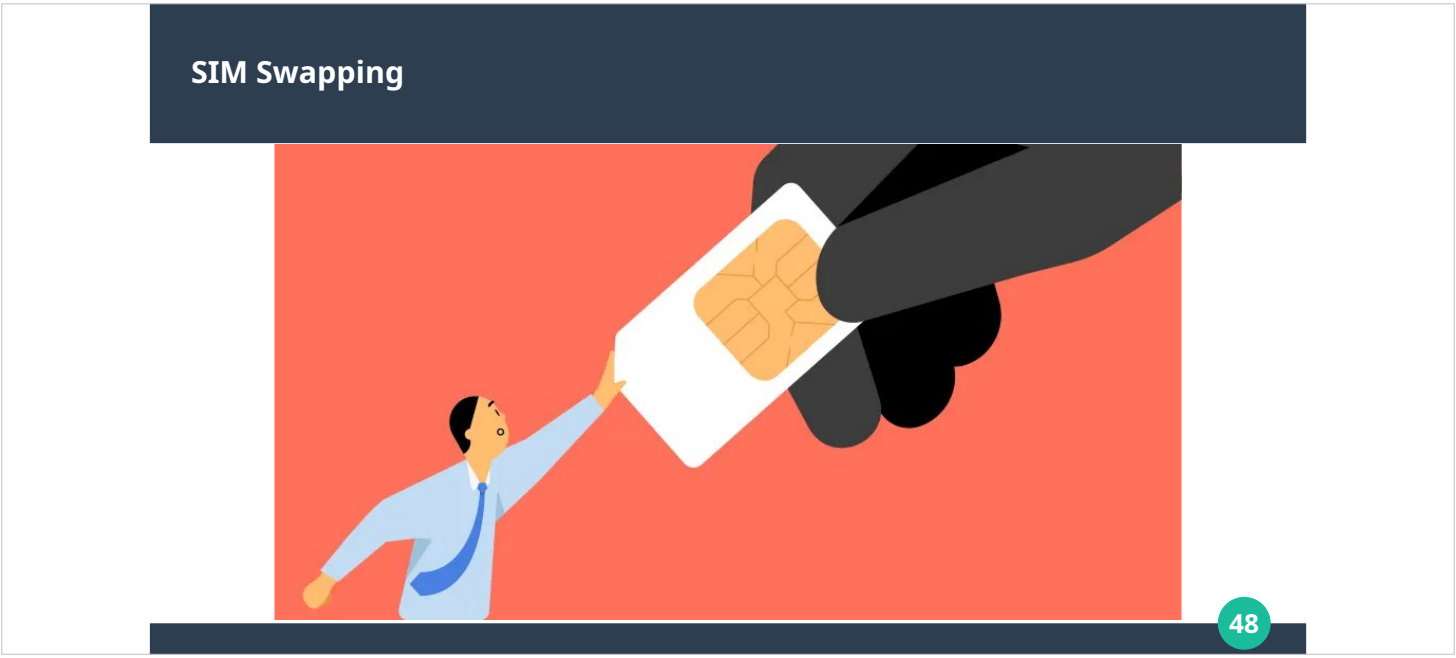

Here’s an advisory from the government of Florida on Identity Theft.
All these articles can be found in the Resources page of the website
LakelandCybersafe.org




We have one more topic to go over before we end the presentation. Let's go back to the big picture diagram from earlier. We just looked at the various aspects of the Internet that matter for cybersafety. Now, we're going to talk about a particular kind of identity theft that may leave a victim confused and clueless for many days before they begin to put the pieces of the puzzle together.

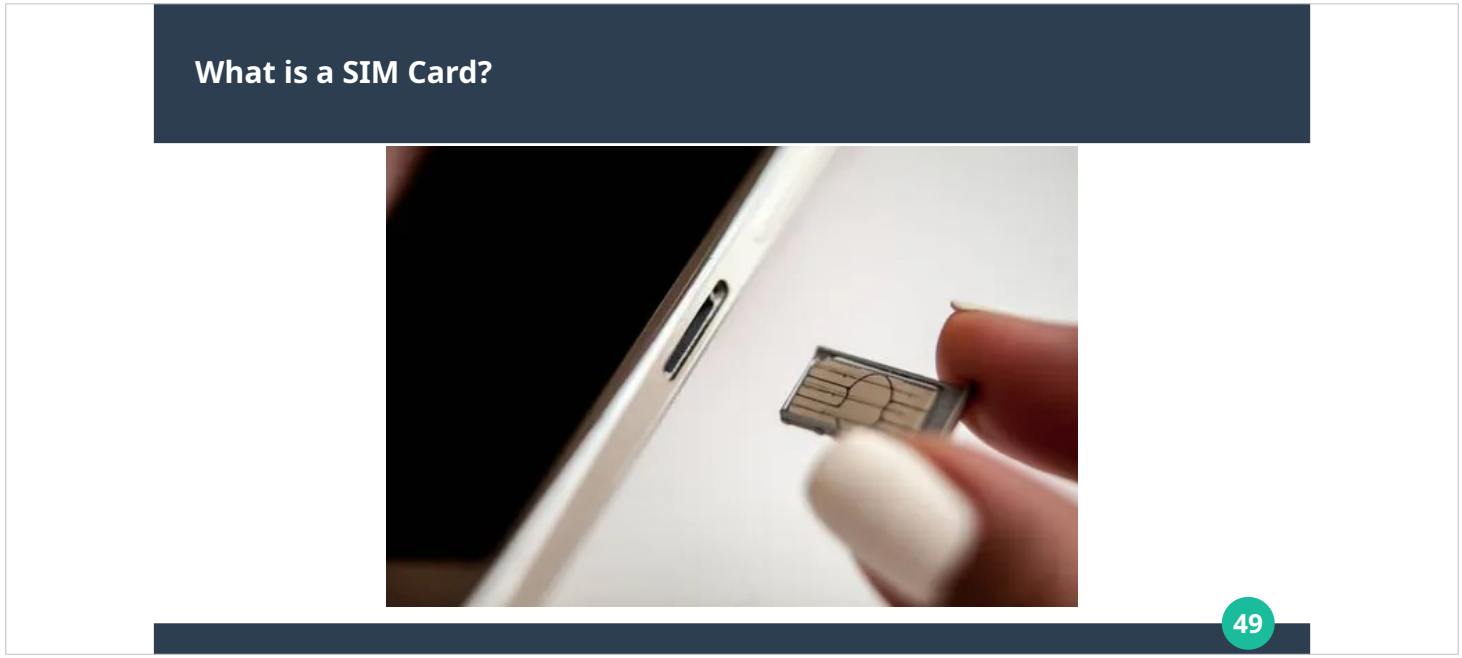
It's called the SIM Swap Scam. The red arrow in the diagram points to a bunch of mobile phone carriers like AT&T, Verizon, T-Mobile, Boost Mobile and Metro Mobile. When we're outside our homes, or if we don't have Internet at home, which is more and more likely the case with younger generations, we rely on the carriers and their cell phone tower infrastructure to connect us to the Internet. Voice, SMS text messages and data are typically included in the same plan.

Whether we have Internet connectivity at home or not, a cell phone plan with data is a practical necessity in much of the world in today's day and age.



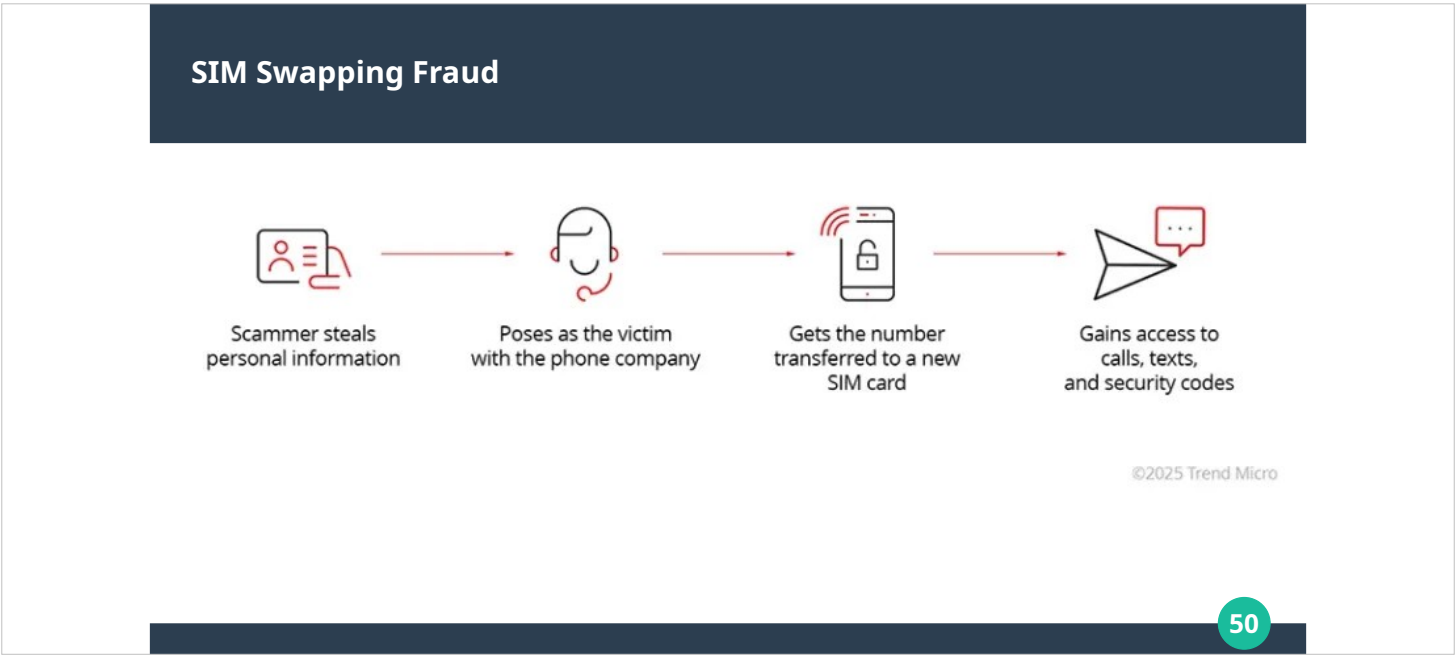

As this picture shows, in a SIM Swap Scam, a scammer hijacks the connection between a mobile phone and the carrier network.

But what is a SIM?




SIM stands for Subscriber Identity Module. If you have your mobile plan with, say, Verizon, the SIM is how Verizon identifies you. It's how a carrier knows to route calls and text messages that are meant for you straight to your phone. Typically, the "identity" part of SIM is a long number that's stored on a little chip like the one shown in the picture. The carrier gives us this chip when we sign up for a plan and we plug it into our phone. From that point on, the phone and our phone number is associated with that SIM card and the phone identifies itself every time it connects to a cell tower.

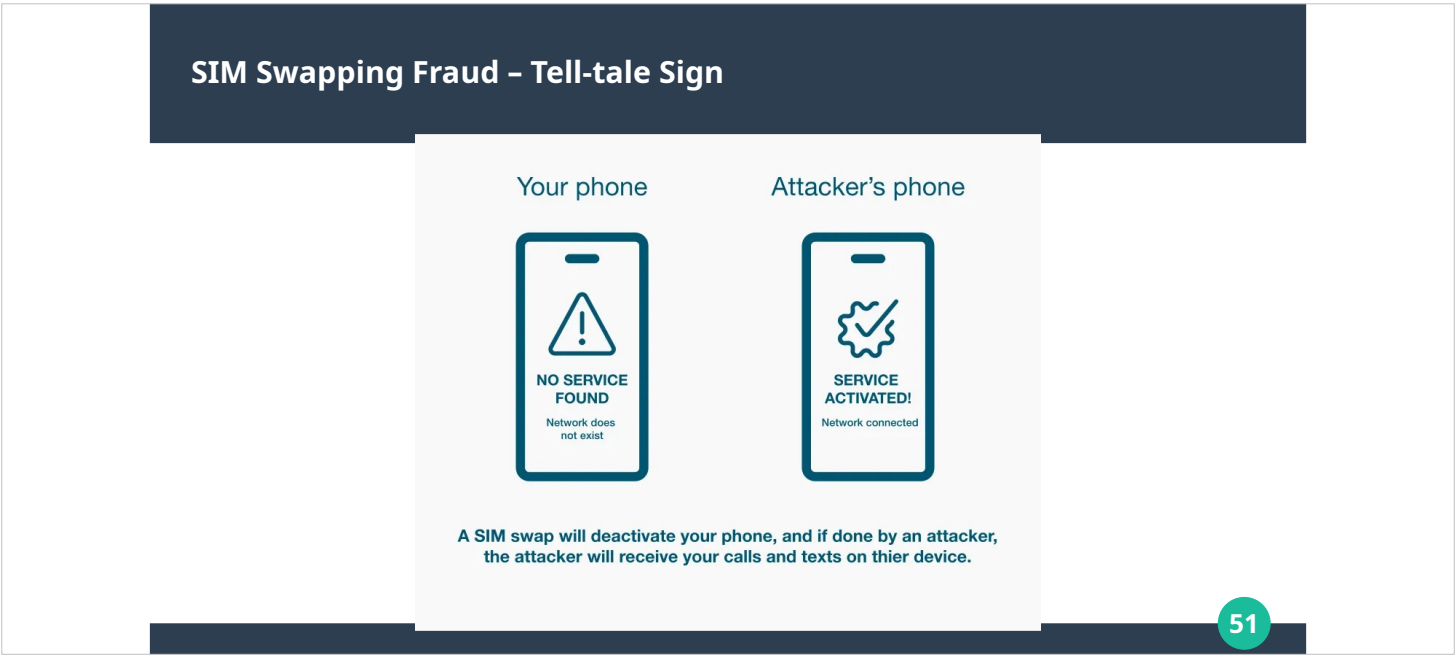
If you have never seen a SIM card, it's likely that your phone was shipped to you with the SIM card pre-installed and set up. Or your phone may have an eSIM which is a digital version of a physical chip. The idea remains the same. It identifies you to the network so the network can locate your phone and beep or ring it when it gets a text message or a call.




In a SIM Swap Scam, this identity is hijacked or stolen by a cyber criminal. A scammer begins with gathering information about potential victims. When he has enough information, including certain identifying information like the Social Security Number, data of birth, and a driver's license number, he is ready to impersonate the victim.

He begins by calling the victim's cell phone company and pretending to be the victim. He might tell the agent that he lost his phone, and now has a new phone that he wants his number transferred to. The words "social engineering" might sound technical, but they mean nothing more than tricking or fooling someone into doing something that they would otherwise decline to do. The customer service agent taking the call of the scammer asks them for personal information, which they readily provide, since they have already done their homework. The scammer knows exactly which pieces of information each cell phone company relies on to verify a customer and he has gathered exactly those pieces. There have been reports that scammers have succeeded in bribing company employees to switch their customers' SIM cards to their own phones. Either way, the scammer now gets a victim's phone number transferred to his own phone.

Now, where do the phone calls and text messages meant for the victim end up? The scammer's phone!

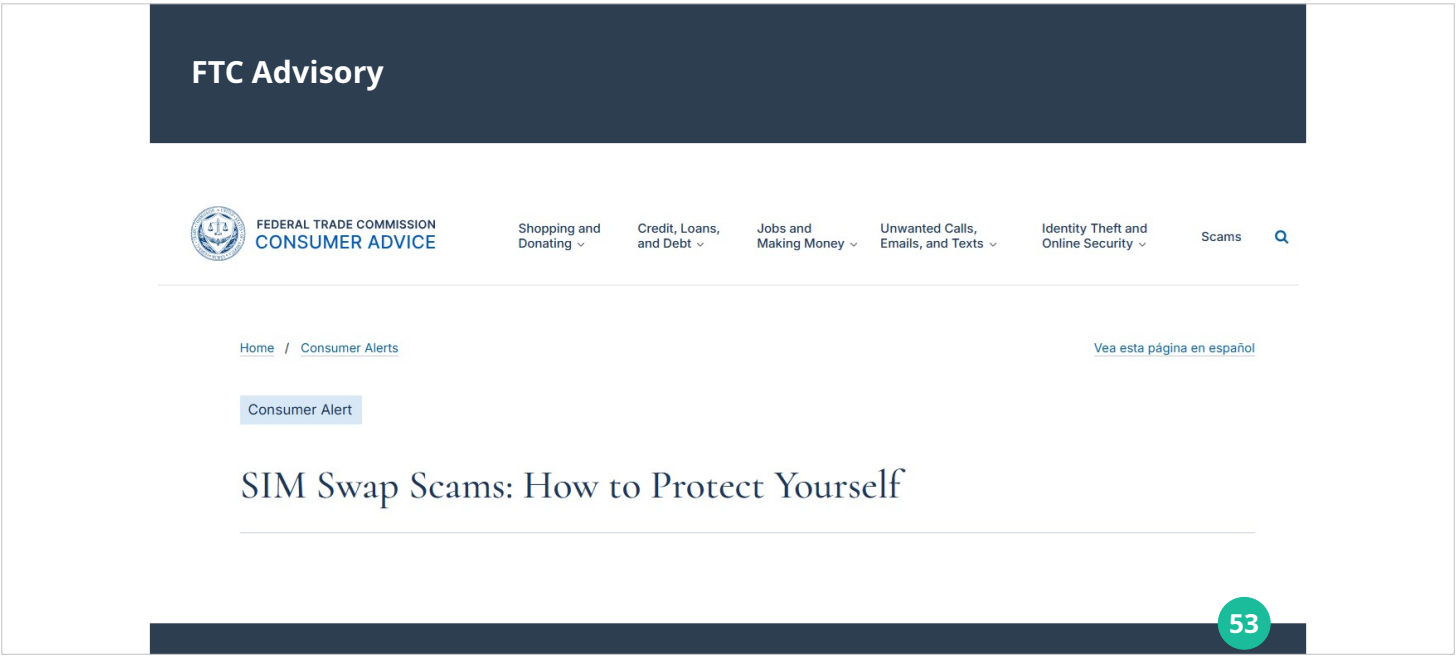



When a victim's SIM is hijacked, their phone loses its connection to the network instantly. This is a sign: if you're going about your day and suddenly notice that your cell phone doesn't show any bars, no signal at all, it's a strong indication that something is going on. A poor signal is a reality in many parts of the world but a complete disconnection from the network is cause for an immediate investigation.

When a SIM is hijacked or stolen in this manner, no one other than the scammer is aware of what's going on: not the victim, nor the cell phone carrier, nor any of the friends of the victim trying to reach them, nor the victim's bank or another institution they have a business relationship with, absolutely no one. The scammer has leveraged the personal information he has gathered about the victim to trick the carrier into handing him the victim's phone number. Now, he leverages the stolen phone number to commit further fraud. He gains access to the victim's online accounts by clicking on the "forgot password" link, and getting the 2nd factor authentication, the text messages with the 6-digit codes, sent straight to his own phone. Or he could use the phone number to first hack into the victim's email account, to which any password reset emails are sent.

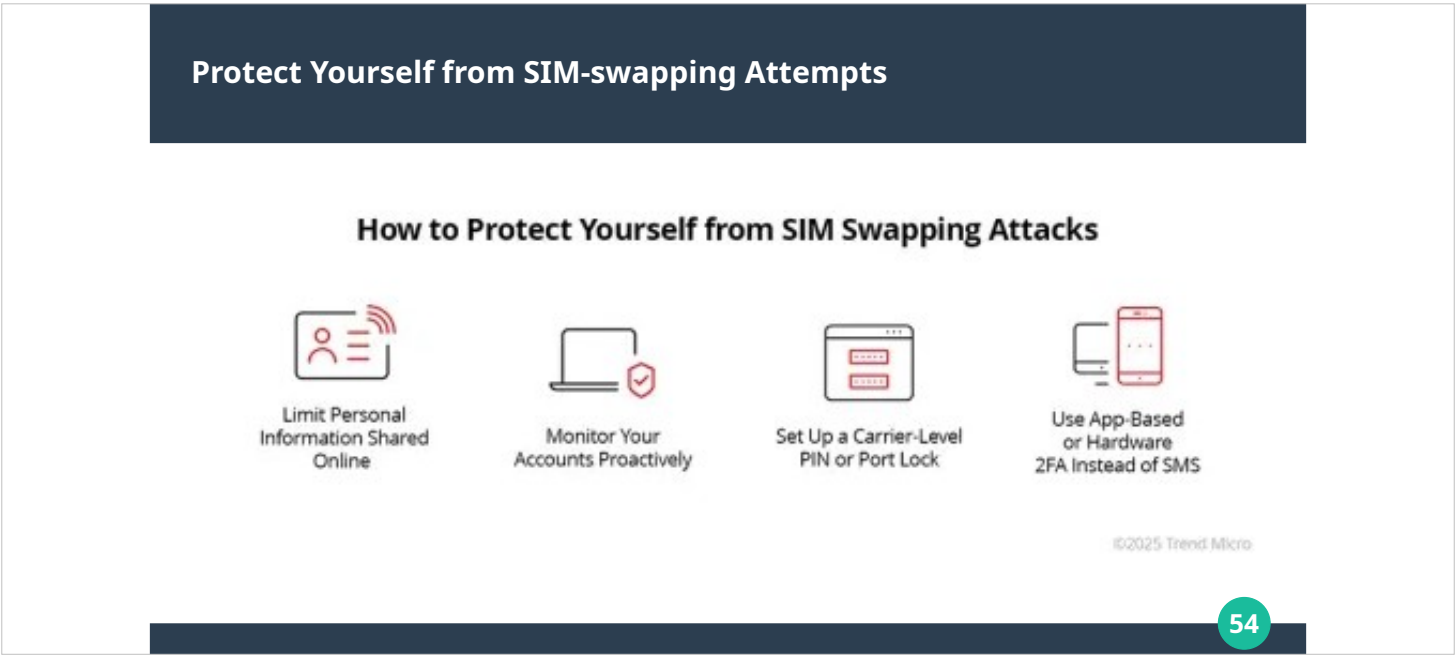

This is an article on the website of the CTIA, which is the trade association of the wireless industry. The carriers, phone manufacturers and others that are part of the wireless industry are well aware of this problem and do their bit to bring about awareness among their customers, but it is an unfortunate reality that the information still hasn't reached many of us.

I personally know someone whose immediate relative has been a victim of the SIM Swap Scam.




The Federal Trade Commission (FTC) has an advisory on their website with tips on how to protect ourselves from a SIM Swap Scam.

We will now talk about some simple steps we can take to get the most effective protection from this type of scam.



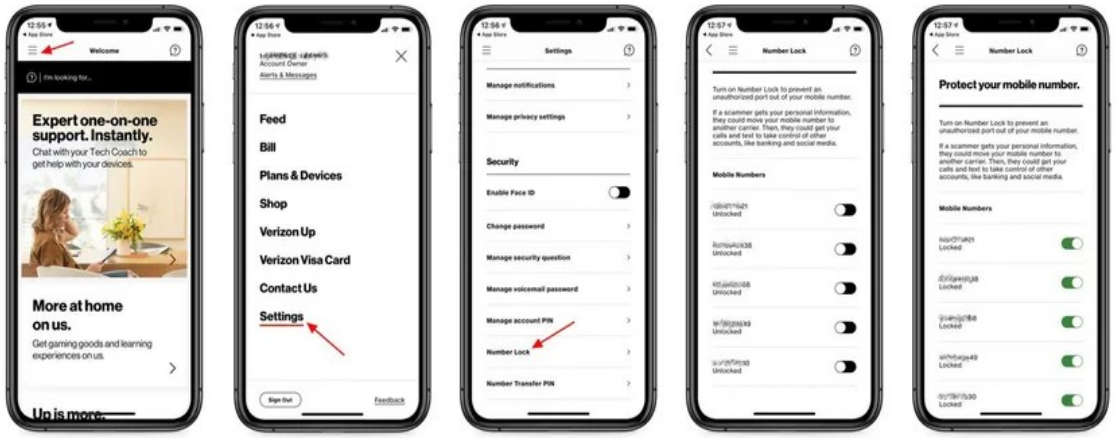

As has been the theme so far in this presentation, limiting the type and volume of information we share about ourselves on the Internet goes a long way in stopping this scam before it begins. Depending on our privacy settings, it's possible for scammers to glean some of the information they need from our social media posts. Then, there's always the Dark Web to buy everything else they need. While we can't do much about the large scale data breaches that happen to big companies where our private personal information is part of the stolen records, we can minimize our contributions to what about us leaks out to the Internet .

Monitoring our credit reports, as we just discussed, might help identity theft from progressing to the level of a SIM Swap Scam.

Setting up a carrier-level PIN that blocks the ability to port out our number is a direct measure we can take to stop a scammer from stealing our phone number. We will look at these settings in the next couple of slides.

To reduce our losses in case we do end up being a victim, we can switch from text-based 2nd factor authentication codes to app-based or hardware-based 2nd factor codes. The latter don't depend on our phone number, so are immune from a Sim Swap Scam. If our bank or

## Verizon Carrier Settings – Number Lock



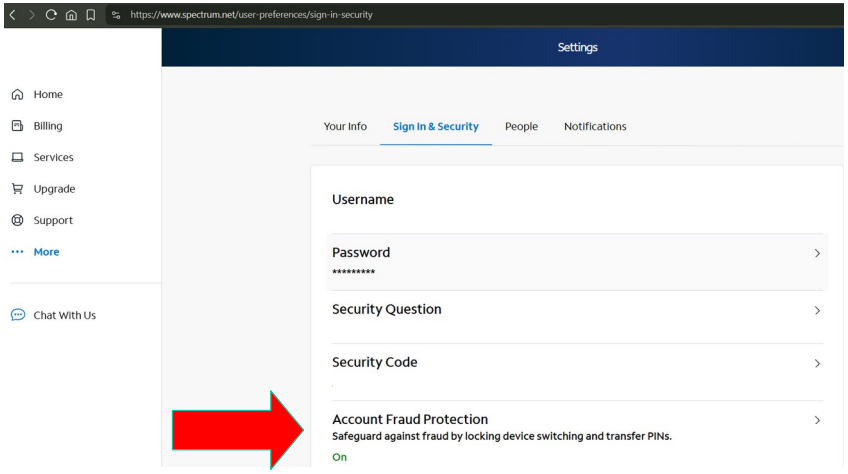

55

Many mobile phone carriers offer this feature. With a port lock or a number lock, once we set it up, no employee or customer service agent of the carrier is able to transfer our number out to another phone without our permission. They need our PIN to transfer our number out, so unless a scammer first hacks into our online account that we have with the carrier, they can't pull off a SIM Swamp Scam. This works for both social engineering and bribery methods.

If we secure our carrier account with a non-text based 2nd factor as discussed in the previous slide, we will have locked down and placed solid protections in place that will guard against this type of scam.

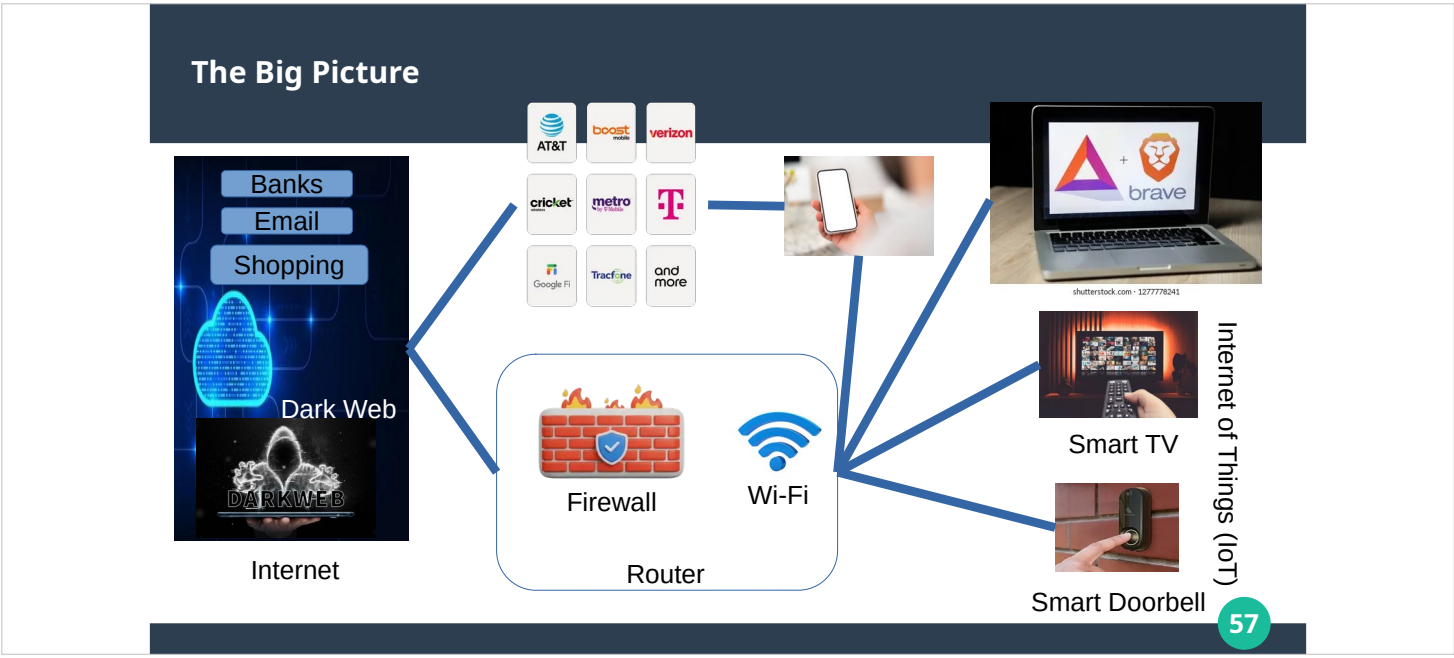
Carriers may call this feature different things, but they are generally available in the security section of the preferences or profile pages of the website or app. The picture here shows the settings on the Verizon app where it's called the "Number Lock".

## Spectrum Carrier Settings – Number Lock




56

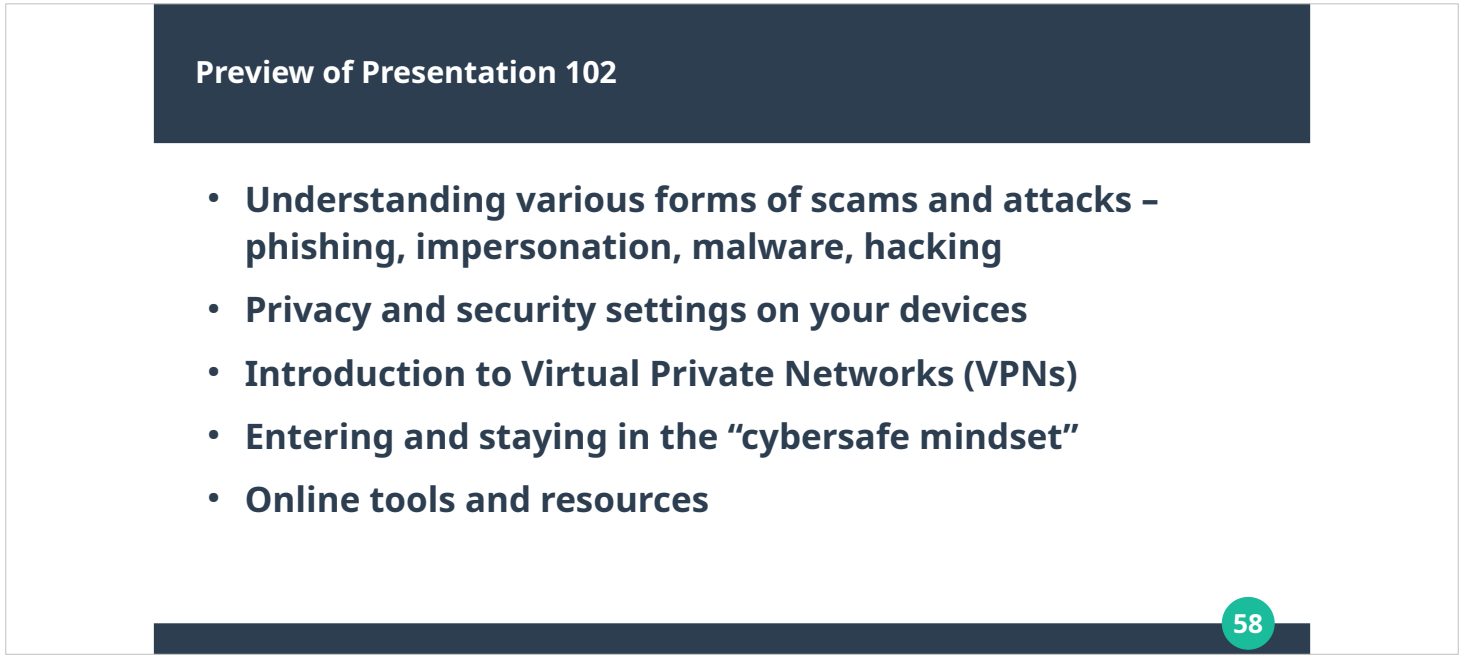
Spectrum Mobile calls it “Account Fraud Protection”. Whether a carrier offers a feature to set up a PIN or not, they generally offer a way to enable the lock.




We go back to the Big Picture finally, once again, to zoom out and see where we have been, where we are, and what we will discuss in the next presentation.

In presentation 102, we will continue looking at the Internet and the many types of scams that spring from the more infamous parts of the World “Wild” Web. That’s at the left of the diagram.

We will also look at the top right of the diagram – computer/laptop and smartphone security settings.




In this presentation, we looked at identity theft and one type of identity theft that happens to be the SIM Swap Scam.

In the next presentation, we will get into the many varieties of other scams such as phishing, and tech support scams. We’ll talk about malware and how to protect ourselves from all these scams.

We discuss anti-malware programs we can install on our computers and phones that will protect us from hackers.

We will briefly touch upon Virtual Private Networks or VPNs which we will cover in more depth in presentation 201.

Entering what I call the “cybersafe mindset” is a theme throughout these presentations and everything we discuss is a part of the journey.

Finally, I point to some very helpful tools and resources that are available online that deal with cybersafety for individuals and families.


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 because these two presentations, presentations 101 and 102, are the basic building blocks of cybersafety that are meant for everyone!

Thank you, again!