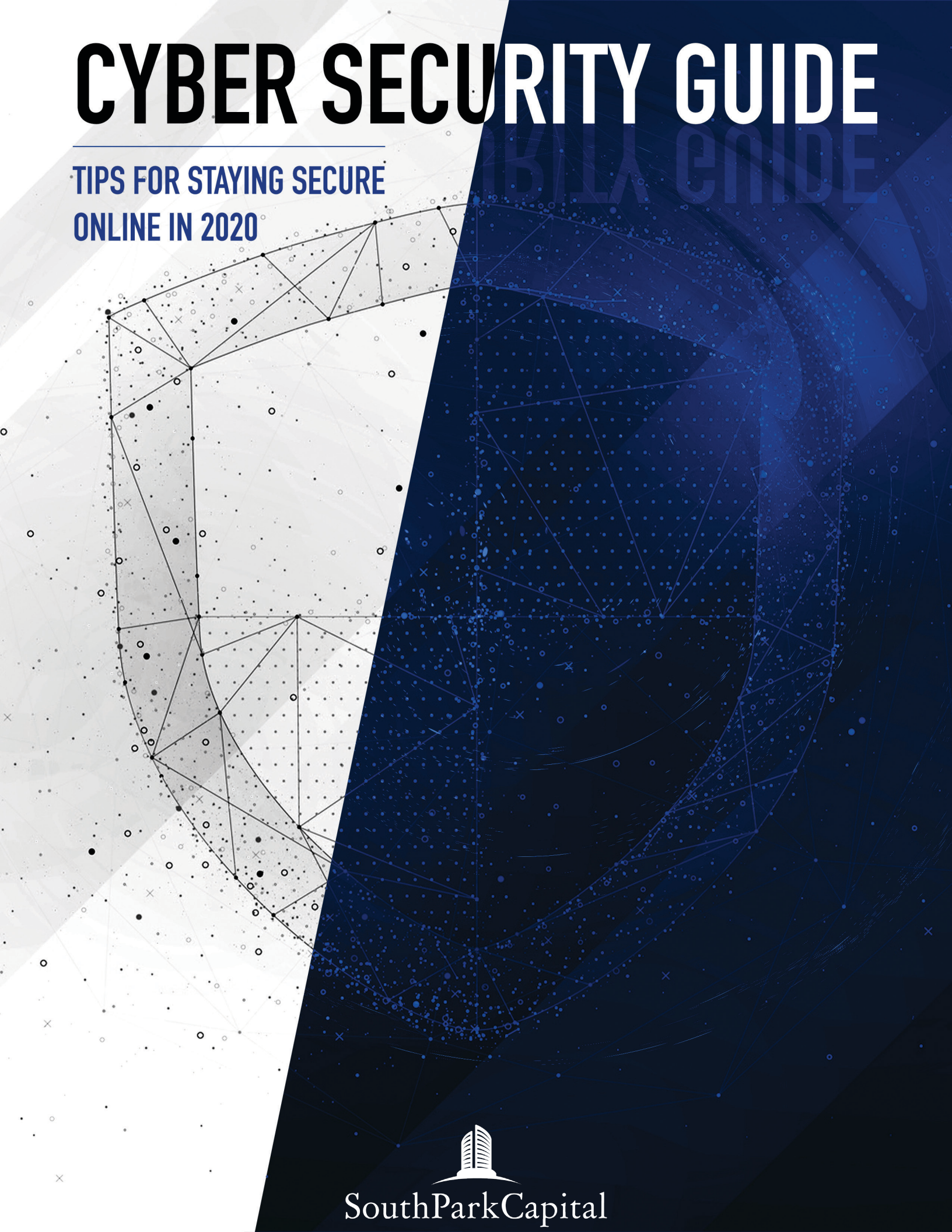
CYBER SECURITY GUIDE

TIPS FOR STAYING SECURE ONLINE IN 2020



SouthParkCapital

CYBER SECURITY GUIDE:

TIPS FOR STAYING SECURE ONLINE IN 2020

Our digitized and networked world allows us to do more things than we may have ever thought possible. Looking back over the last few decades, we have made more advancements in technology than in any other industry. Whether it's to shop, connect with friends and family, manage our bank accounts, or search for information, we spend more and more of our daily lives online.

Unfortunately, while the internet allows us greater convenience and productivity, it also comes with higher vulnerabilities and exposure to risks when it comes to our personal information. Recently there have been multiple events that showcase the dangers of cyberattacks. In July of 2019, Capital One suffered a cyber attack that compromised the personal data of over 100 million customers. This included names, addresses, birthdays, income information, and about 140,000 Social Security numbers.[1]

It's becoming harder for cyber criminals to get ahold of bank accounts, so some are turning to retirement accounts. This is especially dangerous for two reasons: First, people may not check their 401(k) balance as often as they check their bank account, so it could take them longer to realize that something is amiss. Second, if their retirement savings have been stolen, there's no guarantee of them getting it back. Unlike with a stolen credit card, losses to fraud in retirement investment accounts aren't limited by federal law.[2] Think about it – a cyber security attack could mean bigger losses than a market crash. You're concerned about the latter, why not be just as wary of the former?

While there's not much we can do to stop cyber threats entirely, there are certainly ways that we can all be smarter with our cyber-safety.

BEWARE OF THREATS

GADGETS

One of the biggest threats to your cyber security in 2020 is "smart" household devices. Things like Google Home, Amazon Echo, Smart TVs, baby monitors, and smart microwave and fridges that connect to WiFi or Bluetooth can make life convenient, but can also leave you vulnerable. Hacking these devices is on the rise because it's not only a simple thing to do, it's also the last thing you'd think would be hacked. Be sure to do your research and take the proper steps to protect yourself from a very easy hack. The use of "IoT" (The Internet of Things) is becoming more ubiquitous by the day: The number of gadgets connected to the IoT is expected to reach 75 billion by 2025.[3]

Connected devices are handy for consumers and many companies now use them to gather immense amounts of data. However, more connected devices means greater risk, making IoT networks more vulnerable to cyber invasions and infections. Once controlled by hackers, IoT devices can be used to create havoc, overload networks, or lock down essential equipment for financial gain.

SMART MEDICAL DEVICES AND ELECTRONIC MEDICAL RECORDS (EMRS)

The health care industry is going through a major evolution as most patient medical records have moved online and medical professionals have realized the benefits of smart medical devices. However, as the health care industry adapts to the digital age, there are a number of concerns around privacy, safety, and cybersecurity threats.

According to the Software Engineering Institute of Carnegie Mellon University, "As more devices are connected to hospital and clinic networks, patient data and information will be increasingly vulnerable. Even more concerning is the risk of remote compromise of a device directly connected to a patient. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient or disable vital sign monitoring."[4]

Hospitals and medical facilities are still adapting to the digitalization of patient medical records and hackers are exploiting the many vulnerabilities in their security defenses. And now that patient medical records are almost entirely online, they are a prime target for hackers due to the sensitive information they contain.

BEWARE OF THREATS

THE CLOUD

Another potential vulnerability stems from use of the cloud.[5] Even though the cloud can be - and often is - a secure environment, companies and induvial users shouldn't consider it out of sight, out of mind.

As we migrate to cloud-based environments, enterprises and individuals still retain responsibility for the integrity, confidentiality, and availability of that data. Yet all too often, particularly with smaller enterprises, there is some assumption that because they've outsourced their data to Amazon or Google through the cloud, it must be secure. In reality, security depends very much on the company's or individual's cyber security practices.

PHISHING

Be aware of fraudulent phone calls or mailings designed to steal money. Phishing is defined as fraudsters trying to trick you into giving out your personal information by impersonating businesses. A very common cyber-attack targeted at seniors is done through a phone call or letter in which the cybercriminal claims to be a computer company or government agency stating that your computer is broken or that you owe money. Some examples of phishing include phrases like *please verify your account information or it will be deleted, send us your personal information now for a free gift card, or I am stuck in a foreign country and I need $300, please send it at the following link.* All of these tactics are trying to get you to either click a link, provide personal information, or send them money[6]. These are some other common tactics:

- ***Unusual Senders that Appear Credible or Someone You Know:*** For example, if you receive an email that appears to be from Apple or Microsoft telling you that your computer is broken, it's likely not true. These companies wouldn't email you this information or request any personal information online. If you receive an email from someone you do know, be sure that they are not accidentally sending you a virus as well.

- ***Offers That are Too Good to be True:*** An offer may say that you've won the lottery, an iPhone, or some other prize. If it seems too good to be true, it likely is.

BEWARE OF THREATS

- ***A High Sense of Urgency:*** A common tactic among cybercriminals includes a time limit on when you need to take action before a negative consequence occurs. For instance, you may receive an email from someone claiming to be the IRS saying you owe money and it's due by the end of the day or you'll face a hefty penalty. Remember that the government and most companies would not notify you via email (and even over the phone). They'll also likely give you more time and will never ask you for your personal information over the internet. As a general rule, never share your Social Security number or Medicare card number.

- ***Misleading Hyperlinks:*** A lot of phishing emails contain links that may appear to take you to a credible site, like Apple.com, but upon clicking will actually take you to a different site or download a virus. Hover over a link to see the actual destination, and note that these scam emails may also take you to a site very similar to a real site with one letter off like bankofarnmerica.com, for example.

- ***Corrupt Attachments:*** If you receive an attachment that doesn't appear to make sense or is from someone you don't recognize, don't open it. It could contain payloads like ransomware or a virus.

8 THINGS YOU CAN DO TO PROTECT YOURSELF

1 AVOID SUSPICIOUS WEBSITES

You don't have to intentionally download a virus in order to compromise your cyber security. Accidently going to a malicious website can do the job. A malicious website can look like a regular website, but there are signs to look out for:

- *Malicious websites often have poor design quality*
- *They may have many pop-up windows*
- *Their web addresses tend to begin with http, whereas secure website addresses begin with https. (the "s" stands for "Secure".[7])*

To avoid being taken to a malicious website, don't click on emails, suspicious links, or downloads from sources that you don't recognize or if you can't confirm the true identity of the sender.

2 UPDATE YOUR DEVICES

Always make sure that your anti-virus software and computer and phone software remain up to date.[8]

Install the latest version of your web browser. Browsers are regularly updated to help catch scams before they impact massive amounts of people. The most important software to keep updated are your operating system (like Windows, OSX, or your cell phone's software like iOS), your browser (Google Chrome and Mozilla will do this on their own), and your antivirus software. Even if an app update on your phone doesn't introduce many new features beyond "improvements and bug fixes," it's still worth a download from a cyber-security standpoint.

As annoying as the reminders may be, when your phone or computer has an update available, it's important to take the time to install these updates. Updates are made to fix flaws and provide enhancements in a software system or application. While we hope that security researchers discover these issues beforehand, cyber criminals occasionally identify security holes first, but are much more likely to find flaws on an outdated server or application.

8 THINGS YOU CAN DO TO PROTECT YOURSELF

3 KEEP A CLOSE EYE ON YOUR FINANCES

It's important to take a detailed look at your financial statements as soon as they become available to you. Always check statements for inaccuracies and always opt-in for Multi-Factor Identification. Not only is this a good financial habit to get into to assess whether you're paying for things you may not use, but it's an important step in catching fraudulent activity before it has a big impact on your financial security. Double check that your credit card is only being used on purchases that you've made, and if you don't recognize certain purchases, report it to your bank or credit card provider as soon as you can.

4 USE STRONG PASSWORDS

Keeping your finances and financial information private is crucial and it starts with a strong password. Make sure to use random characters when choosing a password. Sometimes creating "passphrases" is more secure than passwords. Having a series of random words in a phrase could be more secure than relying on just one pass "word." And don't fall into the trap of using the same password for all your important personal information.

It's recommended that your passwords are at least 8 characters long and use a combination of upper and lowercase letters and symbols. Try to make your password something that you can remember without using obvious names, numbers, or sayings. There are plenty of password generators and password keepers online to make this process less complicated and to help keep you safer online. Take the following precautions to make sure that your password is safe and protected[9]:

- *Sign up for a password management system (LastPass, Dashlane, RoboForm)*
- *Change your password at regular intervals*
- *Never tell anyone your password, including family and friends.*
- *Lock your screen or log out when stepping away from a computer, especially in a public area.*
- *Use a temporary password when using a public computer or a public network to access confidential information.*
- *Ignore requests by websites asking to "remember" your password.*

8 THINGS YOU CAN DO TO PROTECT YOURSELF

5

USE TWO-FACTOR AUTHENTICATION WHEN POSSIBLE

Many cybersecurity experts have backed this kind of authentication in the absence of a password. Two-Factor Authentication works like this: After going through the usual login process where the user has to enter the username and password, a code is sent to the user's email address or phone number, which in turn has to be logged in. It's a very easy process and typically only takes a few extra seconds to do.

8 THINGS YOU CAN DO TO PROTECT YOURSELF

6

EXCERCISE CAUTION WHEN ONLINE

In this day and age, everyone seems to be on social media. Even though sites like Facebook, twitter, Instagram, and LinkedIn have become norms in our daily lives, it's still important to recognize that we need to stay safe online. Here are some tips on how you can make sure that your information remains private on social media[10]:

- *Make sure to familiarize yourself with the privacy settings on any social media network you use. In almost all cases, you want to make sure your privacy is set to "friends only" so that only people you know can see what you post.*
- *Avoid oversharing about your private life, including full birth dates and places of birth. Sometimes this information can be used by identify thieves and data mining companies. Never share your Social Security Number or Medicare card number online.*
- *Remember that nothing you post online is 100% private. Whatever goes on the internet might eventually be seen by people that are not in your intended audience. Everything posted online can be cached, stored, or copied.*
- *If you use location-based applications or devices, turn location-sharing off.*
- *Always verify that you know an individual before accepting a friend request or a follow. If you receive a connection request from a stranger, it is always safer to decline.*
- *Be sure to log off social media sites after using them to prevent strangers from having access to your account. Always be cautious when using social media sites on public computers.*
- *Keep your phone safe from prying eyes. Make sure you have a password set up on your phone that is unique and hard to guess. Don't use number sequences like your birthday, bank pin codes, or easily guessable combinations. If possible, use a 6+ digit password option or a fingerprint unlocking feature if it's available for your phone.*

8 THINGS YOU CAN DO TO PROTECT YOURSELF

7

TAKE PRECAUTIONS WHEN USING WI-FI AND PUBLIC COMPUTERS

If you're using a public wi-fi network, it could be possible that cybercriminals are attempting to steal information from your computer. It is always important to verify with staff of the establishment you're in that they do have a wi-fi network and that is safe to connect to. Try to avoid doing banking or personal finances on your computer if you are connected to a public wi-fi network.

Never sign in to an unknown internet connection, public WiFi, or a stranger's personal hotspot. Most unlocked "free" wifi connection points are set up to phish your personal information or gain access to your computer. These are especially popular at airports, libraries, and public parks/coffee shops.[11]

Always be sure that your credit card information and passwords are NOT saved on a public computer. A lot of websites offer to save these automatically, but be sure that you click "No" or opt out of this option to avoid giving other people easy access to your accounts. Similarly, make sure you are opting out of the "connect automatically" feature on your wi-fi settings. You can also keep wi-fi off when you don't need it. Even if you haven't actively connected to a network, your computer could still be transmitting data to networks in range. As an added bonus, your battery life will last longer if you turn wi-fi off.

8 THINGS YOU CAN DO TO PROTECT YOURSELF

8

TAKE PRECAUTIONS WHEN USING WI-FI AND PUBLIC COMPUTERS

If you end up the victim of a cyber scam, collect the relevant information about your experience and contact the FBI's Internet Crime Complaint Center (IC3) to file a complaint (https://www.ic3.gov/complaint/default.aspx). One of their analysts will review and research your case and forward the information about the incident to the appropriate law enforcement or regulatory agencies.

It's essential to put measures in place to protect yourself against the many forms of fraud, which include online fraud, identity theft, and Medicare fraud. Here are a few steps you can take:

- *Sign up for auto text alerts and emails of suspicious activity.*
- *Sign up with your bank, credit card company, or third party company (Like Identity Guard) for an Auto Freeze service. This allows you - with the click of a button - to freeze any and all accounts and/or credit cards attached to this service. This can even be used for a lost credit card.*
- *Never give anyone remote access to your computer. Never allow anyone to sign in or do any work on your computer unless you are at a reputable repair shop like the Apple Genius Bar or Best Buy Geek Squad.*
- *Collect mail every day. Place a hold on your mail when you are away from home for several days.*
- *Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.*
- *Ensure the internet service at your house is locked and requires a password to use.*
- *Limit the amount/types of websites you "sign up for." Many websites today are trying to collect user data and those sites are typically easy for hackers to collect a data dump for. If possible, either use the website as a guest or delete your account as soon as you are done with that service.*

NEW DEVELOPMENTS IN DATA RIGHTS LEGISLATION: KNOW YOUR RIGHTS

GDPR

U.S. companies trying to manage regulations and guidance on data protection and cyber security from multiple jurisdictions met an enormous challenge last year when strict new EU rules governing the use of personal information took effect. The European Union's General Data Protection Regulation (GDPR) laid the groundwork for others to follow in passing their own versions of stricter data privacy laws.

GDPR is designed to protect the privacy rights of EU individuals but applies to all companies processing or controlling the personal information of EU residents, regardless of where those firms are located. The regulation took effect May 25, 2018. [12]

A global trend toward stricter or new data privacy laws gathered momentum after GDPR took effect last year. Most noteworthy of these laws is the California Consumer Privacy Act (CCPA), which went into effect January 1, 2020.

CCPA

The CCPA is currently considered the most expansive state privacy law in the United States. In 2019 alone, at least six other states — Hawaii, Maryland, Massachusetts, Mississippi, New Mexico, and Washington — introduced similar privacy laws. Several other states have amended existing laws to include or strengthen data privacy, the use of data, and cybersecurity regulations. Nevada's was one of the first to go into effect on October 1, 2019.

California consumers now have the right to know what personal data a business collects, uses, and sells. State residents also have the right for their personal data to be deleted and not sold. For anyone 16 and older, this is an opt-in situation, but anyone under 16 must give explicit consent to have their data sold.[13]

What if you don't live in California? It's likely that some companies will extend these protections to everyone. However, this might not happen right away as many companies are just beginning the process of complying with this new law.[14] Ultimately, CCPA represents a huge step forward in consumer data protection and you should keep up to date with how it applies to you.

GLOSSARY

- **Antivirus Software:** *These programs protect your computer from Internet viruses or codes that can quickly disable your computer (or an entire network). When functioning properly with all necessary updates, this software will constantly monitor your computer to prevent viruses from "infecting" it.*
- **Bot:** *In the context of cybersecurity, a bot (also known as a zombie) is an Internet-connected computer that has been compromised by malicious code in order to use the computer for something other than what was intended. Bots work together to send messages such as spam or malicious code without it being traceable.*
- **Cache:** *A cache is a technology to store data so that your computer runs faster because it has already done something once before.*
- **Cookie:** *A cookie is a small text file which is placed on your computer when you visit a website. This cookie allows the website to keep track of your visit details and store your preferences.*
- **Extended Validation Certificate:** *Extended Validation certificates are widely considered to be the most trusted option currently available for ensuring the safety of a site. If a site is EV certified, you can rest assured that your information is safe from prying hands.*
- **Hacker:** *A hacker is generally regarded as a person who manages to gain unauthorized access to a computer system in order to cause damage.*
- **Location Sharing:** *Allowing the GPS location of a mobile device to transmit that data to a service. In many cases, users are not aware that location sharing is taking place in their smartphones and tablets.*
- **Malware:** *Short for "malicious software," malware is any program or file embedded into a system to run an unauthorized process for the purposes of capturing information, sabotaging the system, holding it for ransom, or other negative actions.*
- **Phishing:** *A social engineering hack in which the actor attempts to trick a target into delivering access to the target's system. An example of this would be an email message which appears to come from a legitimate address belonging to a bank or major Internet site. The email requests the target enter their login and password or financial information. Don't trust emails asking for personal information.*
- **Spam:** *Spam is made up of unsolicited emails or other types of messages sent over the Internet. Spam is often used to spread malware and phishing, which is why you should never open, reply to or download attachments from spam messages. Spam can come your way in the form of emails, instant messages, comments, etc.*
- **Spoofing:** *Sending an email disguised to look like it is coming from someplace besides its actual origin. The address may be changed, the email address may mimic a known domain, and the email formatting may imitate the design attached to a well-known company or site.*
- **Virus/Worm/Trojan:** *A virus is a self-replicating computer program, designed to be slipped into a computer in order to copy, delete, change, damage, or lock data. A virus frequently uses the infected computer to spread itself to other targets. Similarly, a worm does not alter files, but rather, it stays in active memory and replicates itself. A Trojan or Trojan horse is a virus that appears to have a useful function and uses that shell of legitimacy to avoid security measures.*

CITE SOURCES

1 https://www.cshub.com/attacks/articles/incident-of-the-week-historic-capital-one-hack-reaches-100-million-customers-affected-by-breach

2 https://www.usatoday.com/story/money/2020/01/14/401-k-retirement-accounts-targeted-online/4453891002/

3 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

4 https://insights.sei.cmu.edu/sei_blog/2016/05/10-at-risk-emerging-technologies.html

5 https://www.datacenterknowledge.com/cloud/clouds-cybersecurity-challenges-and-opportunities

6 https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams

7 https://www.consumer.ftc.gov/articles/0009-computer-security

8 https://www.consumer.ftc.gov/blog/2019/06/update-your-software-now

9 https://www.consumer.ftc.gov/blog/2018/03/its-national-password-day

10 https://privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social

11 https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks

12 https://www.consumerreports.org/privacy/gdpr-brings-data-portability-to-us-consumers/

13 https://www.consumerreports.org/privacy/california-privacy-law-ccpa-california-consumer-privacy-act/

14 https://www.consumerreports.org/privacy/california-privacy-law-ccpa-california-consumer-privacy-act/

DISCLAIMER

Securities offered through Arkadios Capital, member FINRA/SIPC. Advisory services offered through Arkadios Wealth. Southpark Capital and Arkadios are not affiliated through any ownership.

SouthParkCapital