

BIZCOM GLOBAL

919-833-8399

[HTTPS://BIZCOMGLOBAL.COM/](https://bizcomglobal.com/)

BizCom[™]
GLOBAL

MANAGED CLOUD, IT & CYBERSECURITY

Cyber- securing Our Future

QUARTERLY

ed. 4

06

THE DARK WEB
LOVES PHI

10

CASE STUDY:
MCNA

16

THE TRUE COST OF
NONCOMPLIANCE

18

WHY REPORTING
MATTERS

21

PROTECT YOUR PII

25

CASE STUDY:
STUDENT LOANS

28

END-TO-END
ENCRYPTION

31

SPAM & SCAMS

34

WHAT CAN YOU DO
TO STAY SECURE?

Security Solutions

INTRODUCTION



Hi!

By picking up this magazine, you've already taken the first step to becoming more cyber-secure in your everyday life! BizCom Global is happy to bring you the latest updates in the cybersecurity industry EVERY QUARTER because the more you know, the better protected you'll be - in your personal and professional life!

Think about the state of the internet when you were born versus where it's at today. Pre-internet and old dial-up computer users remember how it was before smartphones were in every pocket, tracking your every move and helping people navigate every aspect of their busy, modern lives.

Technology is not just here to stay. It is constantly advancing and evolving. How is that changing our approaches to cybersecurity?

That's what we're here to investigate for you.

LET'S GET STARTED

ABOUT US



First, we want to thank you for picking up this magazine and joining the fight against cyber-threats to you and your business! Education is the first (and most important) step toward preventing insider and outsider threats from attacking your personal data.

That's what we do here at BizCom Global!

Since 2003 we have successfully worked with numerous small and mid-sized businesses. Our mission is to provide our customers with constructive technology tools and strategies in order to facilitate improved employee productivity and company growth, while fiercely protecting the underlying organization, its systems, and data, and helping to ensure compliance with the growing number of regulations nationally and internationally.

Bringing you this magazine every quarter is our way of bringing accessible cybersecurity tips and industry knowledge right to your inbox!

LET'S GET STARTED

"True wealth is having your health and knowledge of self."

- *Benjamin Franklin*



THE DARK WEB LOVES PHI

CAN YOU GUESS WHY?

PHI is some of the most lucrative data.

PHI is one of the most valuable types of data on the Dark Web. It can be used for a variety of illegal purposes, such as identity theft, medical fraud and insurance fraud. Although PHI laws initially referred to verbal and physical communication, the digital age guaranteed swift legislation aimed at covering the digital gap.

Dark marketplaces often sell this data in bulk.

By selling PHI in bulk, sellers simultaneously net a bigger sale and simultaneously make it difficult for individuals to track down and remove their own PHI from the dark web. Meanwhile, the consequences of having yours continually available on the dark marketplace can be serious.

PHI affects more than just the healthcare industry.

If you work for a healthcare organization, or even occasionally contract with one (as a lawyer or tech support might), then you MUST comply with health data privacy laws when managing or communicating personal health information. The consequences can be serious—and not just from threat actors, but auditors too!

Yes, theft of PHI really is that dangerous! It can be sold for as little as \$1 or as much as \$1000 for each PHI record, so you need to take care to protect it to the very best of your abilities.

If you believe that your PHI (or any health records that you manage) may have been compromised, you should contact your healthcare provider and the appropriate law enforcement agencies immediately!

When you're taking care of other people's private health information, you need to be vigilant about potential threats to your particular industry and role within the organization.

If your PHI were to end up for sale on the dark marketplace,

- Identity theft can be used to commit fraud, open bank accounts and even obtain credit cards.
- Cybercriminals can use PHI to target individuals with phishing emails or malware that is designed to steal their personal information; the more they know about you, the more convincing the spear-phishing becomes.
- PHI is often used in conjunction with other types of data, such as financial data and social media data, to create a more complete picture of an individual. This information can then be used to target individuals with more sophisticated attacks.

Ransomware, phishing scams, denial-of-service attacks and even insider threats are just as likely and dangerous to your private data as they are to any other industry. There are also many geo-specific laws that may pertain to you depending on where you operate.

Clearly, humans all over the world care about protecting their private health information. That's not the only kind of confidential data that needs to be carefully safeguarded, though. Anyone who handles personally identifiable information (PII) needs to know the industry- and location-specific laws that apply to them in terms of data protection.

Together, we can make the Internet a safer place and keep all of our private data, protected!



PHI LAWS

WHAT IS SECURING YOUR HEALTH INFORMATION AROUND THE WORLD?

United States HIPAA

Health Insurance Portability and Accountability Act (HIPAA) law of 1996 is a United States privacy regulation covering physical, verbal and digital health information assets.

Canada PHIPA

Canada's Personal Health Information Protection Act. There may also be local, provincial privacy laws regarding PHI management, like Ontario's Personal Health Information Protection Act (2004)

European GDPR

The European Union developed the General Data Protection Regulation to protect all EU countries, and it includes specific regulations to protect the PHI of EU citizens. The GDPR applies broadly to any business that processes, holds, or uses European PHI, regardless of the organization's location.

UK DPA

The United Kingdom Data Protection Regulation (DPA) of 2018 establishes rules for how personal data, including PHI, can be collected, used, stored and disposed of. It also requires that they specify to each individual how they intend to use their personal health data.

China PIPL

The Chinese Personal Information Protection Law includes specific stipulations about PHI, including obtaining consent for processing it, limiting the purposes to which they use that PHI, storing and communicating it, etc.

Australia HRA

The Health Records Act (2002) governs the collection, use, and disclosure of health information in Australia. The Act applies to all organizations that handle PHI, including public and private hospitals, medical practices and health insurance companies.

Many global data privacy laws are based on the same fundamental principles, such as the principles of transparency, fairness, and accountability. This harmonization of principles makes it easier for organizations to comply with multiple data privacy laws and for individuals to understand their rights under different data privacy laws.

In short? It helps your company work on contracts abroad, because many of the requirements and controls are the same in these regulations.

Some global data privacy laws even have mutual recognition agreements in place, which allow organizations to transfer personal data between countries without having to obtain additional consent. Cooperation between global data privacy regulators also helps enforce these laws more effectively.

Global data privacy laws are becoming increasingly important as more and more data is collected, used, and shared across borders. By working together, global data privacy regulators can help to ensure that individuals' privacy is protected, regardless of where they live or where their data is processed.

It takes more than a village to keep our data safe and secure—it takes the entire world!



CASE STUDY: MCNA

the PHI leak of Managed Care of North America

Managed Care of North America, commonly known simply as MCNA Dental, suffered a major healthcare data breach when its systems were infected with malicious code.

On June 26th, 2023, an unauthorized party was able to access systems and remove copies of personal information, including the protected health information (PHI) of 8.9M patients under their care.

The compromised PHI included names, addresses, telephone numbers, email addresses, birth dates, Social Security numbers, driver's license numbers, government-issued ID numbers, dental benefit information, and health insurance information.

This is just one example of a recent case of PHI being stolen from a health organization!

In 2023 alone, PHI breaches affected...

- 11M patients of HCA Healthcare, the largest health system in the United States.
- 1.7M patients at the University of Michigan Health Service and School of Dentistry.
- 25.5K patients at the internal medicine practice, ASAS Health, in Edinburg, TX.

As the healthcare industry becomes increasingly digitized, it is more important than ever for healthcare organizations to take steps to protect patient data.

Of course, as we know, there are numerous legislations around the world aimed at protecting your physical *and* digital PHI.

”

HEALTHCARE
ORGANIZATIONS
... SHOULD TAKE
CARE TO
PROTECT
PATIENT DATA.

The healthcare organizations to which you entrust your PHI should take care to protect patient data. They might use strong security measures, educate workers about cybersecurity best practices, regularly back up and test important data, and have an incident response plan in place.

Sound familiar?

Just like those in the healthcare sector, YOU have to protect the confidential data on *your* systems. Whether that's your own or others', you are responsible for its secure management and communication!

While you may handle different *kinds* of data, the lesson here is the same: We all want to believe that when we entrust our private data to someone, we expect them to keep it...well, private.

\$9.3 MILLION

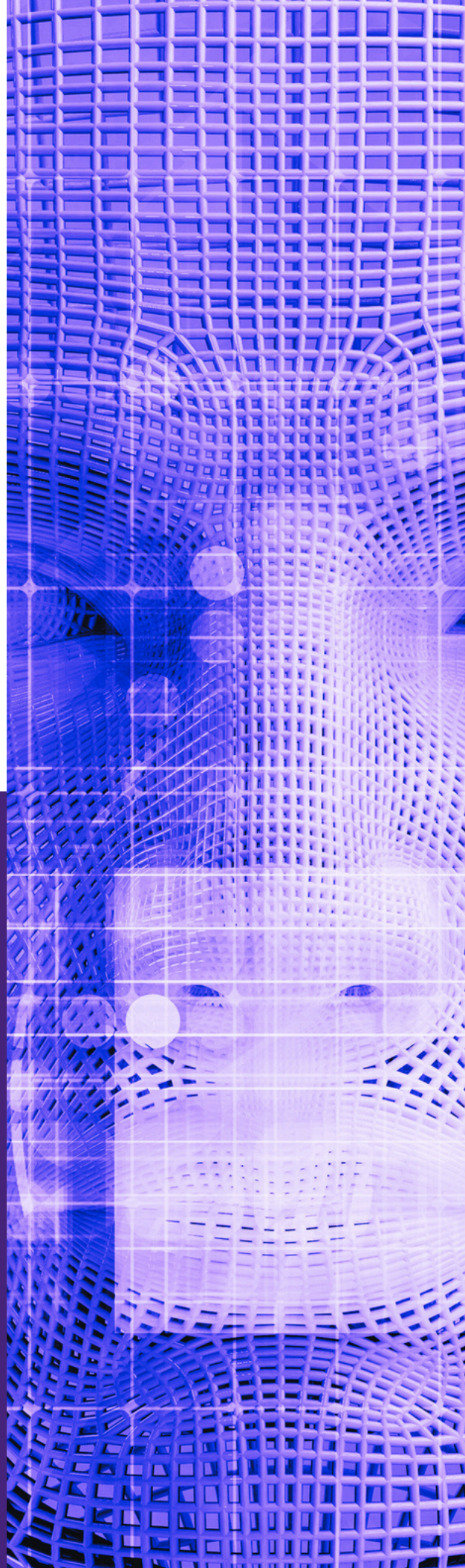
This is the average cost of a data breach in the healthcare industry, which is a higher average than any other industry,.

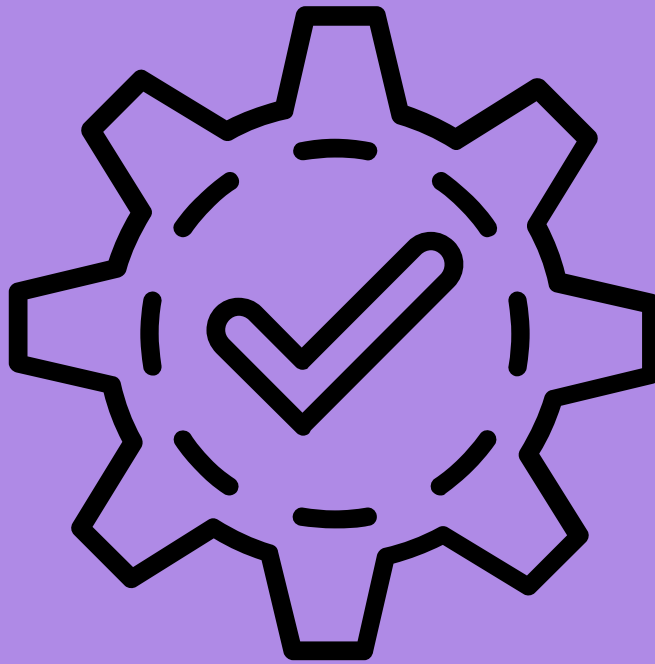
89% OF HEALTH ORGS

That's how many report *an average of 43 cyber attacks per year*. It is the most targeted industry for cyberattacks.

95% OF IDENTITY THEFT

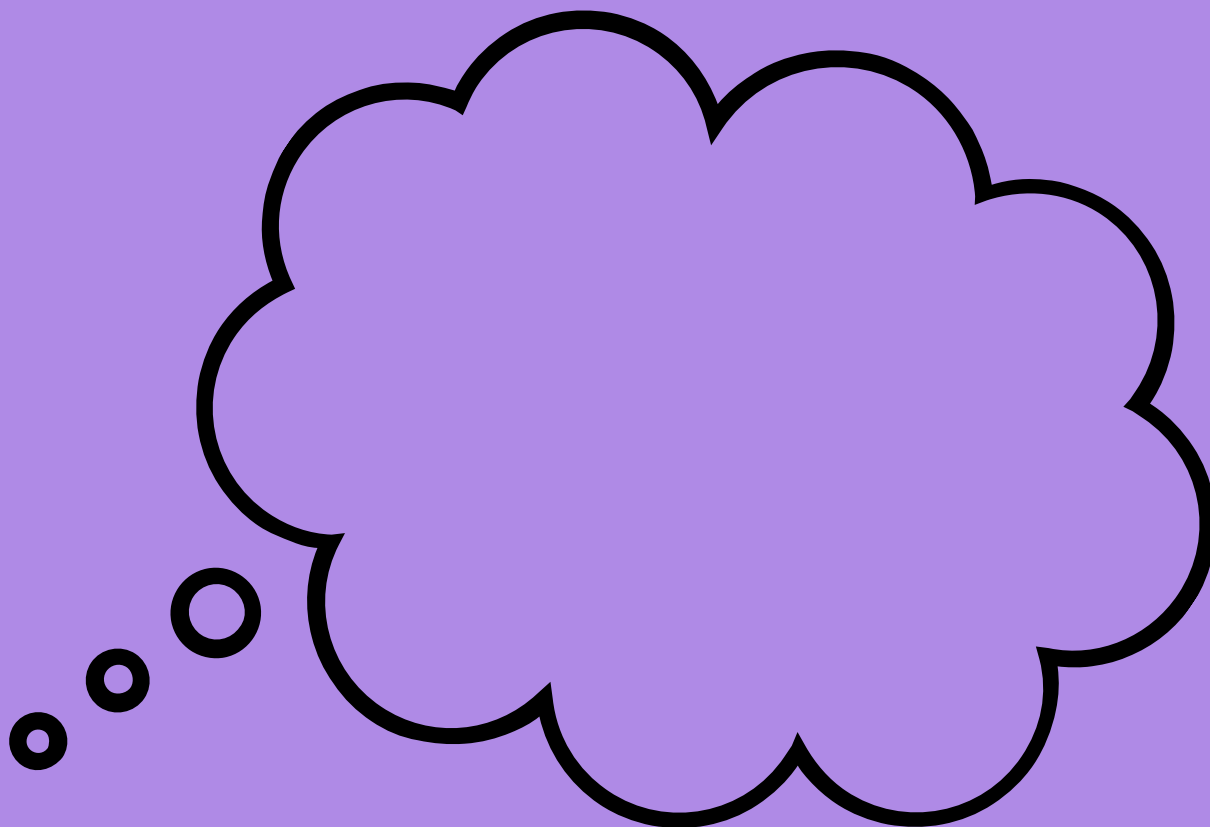
Stolen healthcare records are the most common way to commit identity theft.





**"True cybersecurity is preparing for what's next,
not what was last."**

- Neil Rerup



WHY CYBER COMPLIANCE REALLY MATTERS

57%

More and more companies are recognizing the importance of following cyber-compliance regulations. Now, over half of organizations plan to dedicate more time to risk management, 22% more than last year.

\$10K

The estimated cost of getting a single employee up to standard with compliance regulations is \$10,000. Some of this cost can be mitigated with documented procedures for onboarding and all training.

66%

Depending on the size of your organization, getting every employee up to speed with compliance regulations can become quite costly. 66% of companies cite compliance as the main driver of extra spending!

\$14M

After totaling up the fines associated with noncompliance, legal fees, penalties, loss of profit and productivity, and other disruptions to the daily workflow - noncompliance costs more than \$14M overall.

70%

When organizations properly train their employees about security awareness and cyber-compliance, it decreases the odds of a data breach drop by 70%! Cyber-compliance isn't just necessary...it's smart.

IT'S NOT JUST LEGALESE AND FINES!

No matter what industry that you work in, there are undoubtedly *some kind of legislation* surrounding best practices for protecting private data and the confidentiality of your clients. You can't just walk into a doctor's office, proclaim you're someone's sibling and start demanding medical information!

Compliance regulations aren't designed to make your job more difficult. It helps to protect individuals and organizations from harm. For example, businesses that comply with health and safety regulations are less likely to have accidents that injure or kill their employees.

Second, compliance helps to maintain fairness and equality. For example, data protection laws help to protect everyone's privacy regardless of their demographics or wealth.

Third, compliance can help to build trust and reputation. For example, customers are more likely to do business with companies that they trust to comply with the law.

Compliance is an important part of our society. By complying with rules and regulations, we can help to create a safer, fairer, and more prosperous world for everyone.

Ultimately, cybersecurity compliance matters because it takes ALL of us to create a more secure digital landscape where we can coexist safely.

If you are blasé with your customers' data, and your own cybersecurity in general, then there's a much higher chance that you will fall victim to social engineering scams and open your systems to data leakage and theft.

It's like the Golden Rule we all learned in kindergarten: ***Treat others' data the way you want yours to be treated!***

You don't want YOUR *personally identifiable information* to end up on the Dark Web...well, your clients don't either!

Of course, it goes beyond the dangers associated with security incidents; slip-ups that lead to data breaches can affect your job, land you with massive fines, and even get the law involved.

So next time you're wondering if cyber-compliance is really that important, you'll be able to answer that question with a resounding YES.



3 LAYERS OF CYBER-COMPLIANCE

1. REGULATORY COMPLIANCE

These are broad regulations which are imposed by *external* agencies, like government departments or industry associations. At its essence, all this means is that you must abide the external rules set upon your industry and job. For example, businesses must comply with health and safety regulations, data protection laws, and environmental regulations.

2. CORPORATE COMPLIANCE

This refers to compliance with internal rules and policies, such as those set by a company's board of directors or management team. For example, companies may have policies on ethics, conflicts of interest, and insider trading. While these regulations aren't set in stone via legislation, they *are* part of your contract and agreement to work with your employer.

3. INDIVIDUAL COMPLIANCE

Oftentimes, we have to keep ourselves in check and follow social and interpersonal rules set upon us. We may have these expectations set by others, such as parents, teachers, or employers. For example, children are expected to comply with their parents' rules, and employees are expected to comply with their employers' policies! Even if eyes aren't on you at all times, you're expected to be self-sufficient.



THE TRUE COST OF NONCOMPLIANCE

*what does it matter,
aside from the legalities?*

Failing to abide by cyber-compliance best practices can have serious consequences for both individuals and organizations—and it's not just because of the fines and other penalties that come along with noncompliance.

First and foremost, noncompliance makes it much easier for cybercriminals to steal sensitive data, such as personal information, financial records, and intellectual property. By following best practices, you are actually *avoiding* identity theft, financial fraud and other damages to you and your organization!

Consider what's at stake if a breach on your organization led to the theft of your PII alone. HR has your Social Security number, information for direct deposit or direct mailing, your full name and birthday...

You don't want all that up for sale on the Dark Web!


Keep in mind that the legal and financial penalties associated with noncompliance are no joke. It's not just the regulatory agency that you must face, but potentially lawsuits from individuals whose information was leaked in the breach.

There are also damages to your reputation to consider: Would you trust a service that continually leaked your data, all because they regularly failed to comply with common industry regulations? Probably not!

With lost trust comes lost business, and compounded concerns from any investors.

Whether you manage a whole organization, small team or just the data on your own systems, cyber-compliance is a team effort. We ALL benefit from following regulations.

Ultimately, noncompliance makes your systems much more vulnerable to cyberattacks of all kinds. Best practices aren't just so that you can tick off a checkbox; they're set in place to keep us all safe.

A person wearing a dark hoodie is seen from behind, sitting at a desk. In front of them are several computer monitors displaying code or data. The scene is dimly lit with a strong blue light source, creating a high-tech, cyber-themed atmosphere.

"The biggest threat to cybersecurity is not technology;
it's people."

- *Kevin Mandia*

WHY REPORTING MATTERS

Have you ever experienced a cyberattack, either aimed at you or leveled at your organization?

If so, then you might already know how important it is to report the breach...and we don't just mean to your direct managers or the police (although, depending on your organization's incident response plan and your role in it, you might have to do that too)!

When a data breach happens, you are often beholden to laws detailing what, how fast and to whom you must disclose. For example, financial institutions have to notify the Federal Trade Commission within thirty days. You typically have to disclose the breach to anyone affected, too, depending on what information was stolen.

Reporting is one of many important regulations that make you more cyber-secure. Think about it: If your bank accounts, or health records, or mailing information got leaked, wouldn't you want to know?

It's not just about preferences, though...data privacy is a right in many countries across the globe! More and more, people and legislation are all pushing for better data privacy protections.

Did you know? There are 162 data privacy laws in place around the world! Some are focused only on your locale, while others apply to the whole nation. We even have international relations updated to consider how much digital communication goes on now.

How can we keep our accounts and data private if we don't know when a breach has occurred? If you don't know YOUR reporting requirements, now is the time to found out!





Promptly notifying affected individuals allows them to take proactive measures to safeguard their compromised information, like changing all of their passwords or Dark Web Monitoring software, like ours, that delves deep into the dark marketplace to instantly detect your compromised information.

Ultimately, reporting matters after a breach because it mitigates damage from the breach and teaches us where to improve. When alarm bells are rung, authorities and experts can work together to identify the source of the breach and take action to improve security measures for the future.

“Ultimately, reporting matters after a breach because it mitigates damage from the breach and teaches us where to improve.”

Transparency is also key to maintaining your upstanding reputation. Who wants to be known as someone who hides massive privacy breaches from the ones who are most affected? Organizations that openly acknowledge and address data breaches demonstrate transparency and accountability to their customers, partners, and stakeholders. This transparency helps maintain public trust and confidence in your commitment to data security and privacy.

So it really does come down to the age-old good advice: ***If you see something, say something!***

WHEN THE DARK WEB DARKENS YOUR DOOR

If your data is leaked in a security breach, it's very likely to end up misused or up for sale on the dark marketplace.

When you have Dark Web Monitoring software, it automatically notifies your managed service provider about your personally identifiable information (PII) showing up illegally. That way, incident response plans can kick off immediately.

2.5M

people trawl the dark web every single day, and over half are already criminals

More than half of the people who traverse the Dark Web every day are estimated to have already done something illegal. It's not just the number of people browsing the Dark Web, it's their seasoned history of criminal behavior which suggests they know what they're doing when it comes to digital threats.

So.....who's looking to buy or sell YOUR *personally identifiable information*?

PII on the Dark Web sells for average of:

- \$15 per credit card number
- \$20 for driver's license information
- \$2000 for your passport
- \$15 for a Social Security Number
- Up to \$1000 for personal health information (PHI)



PROTECT YOUR PII

| 80%

*of data
breaches
contain PII*

| 1/3

*of Americans
have faced
identity theft*

| \$4M

*is the average
cost of a
data breach*

- Be careful about where you enter your PII online. Only enter your PII on secure websites, which use HTTPS instead of HTTP.
- Use strong passwords and enable two-factor authentication whenever possible.
- Be careful about clicking on links in emails or on social media. These links could lead to phishing websites that are designed to steal your PII.
- Keep your software up to date. Software updates often include security patches that can help to protect your devices from malware and other cyber threats.
- Be aware of the latest cyber threats and scams. Make sure to read the news and follow security experts on social media for updates on the latest cyber threats.



BEATING CREDIT CARD THEFT

IT'S SUPRISINGLY COMMON...
AND COMMONLY LEFT
UNDEFENDED!

Digital wallets, pervasive online shopping trends, near-field communication and the fast-paced world of technological invention all make using your credit cards more convenient, but it puts your financial data at risk, too.

Thankfully, we can enjoy the ease of use without sacrificing our data's security in transit and storage. For example, if you have multiple credit cards, you should ALWAYS use different log-in credentials for each one. A hacker might sacrifice one, but that doesn't have to spell danger for all of your other cards, too! You can better ensure your banking information's safety by...

440K

*# of credit card
fraud reports
filed in 2022*

- avoiding public WiFi, where anyone can spy on your browsing
- immediately updating software with unpatched zero-day vulnerabilities
- not saving credit cards to your web browser
- using antivirus softwares and web scanners that notify you about unsafe sites
- avoiding suspicious links and uncharacteristic messages from your bank or other financial institutions

When in doubt, always go directly to your preferred financial websites instead of clicking links that accompany messages pressuring you to act quickly. Your financial information is precious; take as good a care of it online as you do of the physical cards in your wallet.

Being careful can only get you so far. Sooner or later, you'll lose focus for a second or someone will devise a crafty enough trap to trip you up. You had better hope that your accounts are secure enough to withstand their attempts to break in!

Every technical advancement that humans make is a double-edged sword: While daily life becomes more convenient with each step forward, it provides more chances for cybercriminals to steal your data. If your credit card is connected to your digital wallet, for example, then hackers don't have to take the card from your pocket or memorize the CVC code; they can opt to go after a vulnerability in the storage system that houses your digital wallet's information. If your phone gets stolen, and you don't have a PIN, that would be another way for a criminal to access your bank funds illegally (doubly so if you don't sign out of your banking app after each use!).

Multi-factor authentication (MFA) requires several forms of identification to let you into an account, for example, in addition to a password you might sign in with a one-time passcode (OTP) connected to an authenticator app, SMS messages or emails; face or fingerprint scans, or voice recognition; a PIN or whatever other kind of MFA your banking apps can set up.

In 2021, there were approximately 390,000 reported cases of credit card fraud. In 2022, such reports exceeded 440k. In just the first half of 2023, officials received reports of nearly 220K such fraud cases.

While credit cards are a useful tool to have in our (digital and physical) wallets, they aren't foolproof! These simple steps can help keep your accounts safe from hackers and thieves.



PII VS IDENTITY THEFT

Identity theft is one of the fastest-growing crimes in the world. Every year, millions of people have their identities stolen, which can lead to significant financial losses and damage to their credit scores.

How does identity theft happen? When your *personally identifiable information* is compromised, cyber-thieves can use that information to impersonate you in various scenarios—and if they do it right, they can successfully steal your identity.

Did you know? The U.S. Federal Trade Commission estimates that 33% of people have been the target of attempted identity theft. Considering that the crime costs victims an average of \$4,957 (*Javelin Strategy & Research*), this can be a worrying figure. That's not enough to mention the years of phone tag you could end up playing with the IRS!

Still, the question remains: *Why* do cybercriminals want to steal your PII and, ultimately, your identity?

Everyone has their own motives, but commonly, identity theft is committed to gain government or health benefits; illegally get employment; conceal or frame you for their criminal activities; blackmail. or pure financial gain.

Identity theft can have a serious impact on your finances, credit history, and reputation. It can take months or even years to recover from identity theft.! Protecting your PII is critical to avoiding cyberattacks and all their repercussions.

Protect yourself from identity theft!

- Be careful about what and to whom you share information with online.
- Shred confidential documents before you throw them away.
- Use strong passwords and multi-factor authentication for your accounts.
- Monitor your credit report and bank statements for unauthorized activity.
- Be aware of the signs of identity theft, such as receiving bills for items you didn't buy or getting turned down for loans for no apparent reason.

If you think you have been a victim of identity theft, report it to the police and the Federal Trade Commission (FTC).

CASE STUDY: STUDENT LOANS

\$ 1.78T

Did you know? When 2023 began, student debt across America had reached a staggering \$1.78T in total. Individuals owe over \$37K in federal loans alone.

Are you among the 43M who owe student loan debt in America? Then you've probably heard about the Supreme Court decision from June 30th, which struck down President Biden's attempt to forgive approximately \$430B in federal student loan debt. ***That's 43M people who were expecting tens of thousands in debt relief.***

Unfortunately, student loan givers and takers weren't the only ones to hear this news... Scammers know about it, too.



Most student debt in the United States is a federal loan; in fact, **private loans only account for approximately 8% of what's owed** across the country.

Why does that matter? Well, because it's easier to send a mass email to scam targets if there's a higher likelihood that they one, owe money from higher education; and two, took out federal rather than private loans. It increases the chances that the targets will fall for the phishing "bait."

Geographically, it breaks down even further: New Hampshire, for example, has the highest amount of debt per state, closely followed by Delaware and Pennsylvania. Scammers may choose to focus on those areas to try and get a bigger payout. Alternatively, they may go after Washington D.C. student borrowers because they have the highest national balance.

Narrower parameters can mean a more specific and personalized message, which can often be more effective in convincing victims to send money or information. Phishing continues to be one of the most effective ways to steal your information.

HOW TO SPOT DEBT RELIEF SCAMS

- **Be wary of upfront fees.** Always be cautious if someone asks for payment before providing any services!
- Scammers often make unrealistic promises, like immediate loan forgiveness or significant debt relief. Remember that there are no quick-fix solutions for student loan debt. **Be skeptical of any offer that sounds too good to be true.**
- **Do not share personal information**, such as your Social Security number or FSA ID, with unverified entities. Scammers can use these details to commit identity theft.
- Stick to reputable sources when seeking assistance with your student loans. Start by contacting your loan servicer or the official government websites, such as the U.S. Department of Education's Federal Student Aid (studentaid.gov), to **explore legitimate options** for loan repayment or forgiveness programs.
- Scammers often reach out via **unsolicited phone calls, emails or texts**. Legitimate organizations don't initiate contact without your consent.



- If you get that “gut feeling” about a message, **trust your instincts**. Take time to carefully evaluate any services related to your loans. Don't be rushed or pressured into making immediate decisions.
- Take the time to research and verify the legitimacy of companies offering student loan assistance. Check their website, look for reviews or complaints, and confirm their contact information.
- If you have doubts or concerns, reach out to trusted sources for guidance. Consult with your loan servicer, financial aid office or a reputable financial advisor who can provide you with reliable information and advice.

Remember to stay vigilant, ask questions, and verify the legitimacy of any student loan assistance programs.

"Cybersecurity is a team sport."

- *Michael J. Keegan*



END-TO-END ENCRYPTION

Are YOUR messages safe?

Even if you use encrypted databases and secure communication methods, they might not be secure. Did you know that hackers can still read messages once they've broken into the system that holds them? It's true.

What about when you're sending those same messages out into cyberspace? Are they free from prying eyes there?

No...not unless they have end-to-end encryption. The best communication channels employ this tactic so that your messages aren't just protected at rest...they're safe from hackers when they're on the move, too.

End-to-end encryption secures the confidential servers and messages so that the data must be *decrypted* before it can be accessed or viewed...even in transit.

Why does end-to-end encryption matter?

This hyper-secure communication method ensures that your private conversations remain confidential. Even if a third party gains access to the servers of the messaging app, they will not be able to read your messages.

When a hacker intercepts, views and/or modifies messages that are being sent between two parties, it's known as **man-in-the-middle attacks**. You can imagine the damage that could be done if you think you're sending and receiving accurate, confidential information with someone trustworthy—and no one else.

Encrypted messages, meanwhile, are unreadable to anyone without the decryption key...even when that information is stored in your inbox or data logs. It helps prevent your data from access by any unauthorized party, no matter when they try to break in. Even if they manage to get onto your systems, they won't be able to read anything.

End-to-end encryption protects your privacy so that even if your network is broken into, or someone hacks your device or that of the person you're communicating with, all your data will still be secure. Already, we see technology like this implemented in applications like WhatsApp, Signal and Telegram to name just a few.

If you are concerned about the privacy of your online communications, end-to-end encryption is the answer! It's a safer and more secure way to ensure the integrity of your online accounts and communications remains intact.



DID YOU KNOW?

35%

increase in successful man-in-the-middle attacks this year

Source: Cofense Intelligence

94%

of web traffic in 2023 is encrypted thanks to the rise in HTTPS://

65%

of organizations have encryption services in place

50%

of man-in-the-middle attacks aim to steal log-in, banking and other confidential information

SPAM TAGS & FILTERING

Sick of getting spam emails?

You can actually add spam tags to help filter out unwanted emails that their built-in spam filters aren't catching.

If you notice that you've been getting a lot of spam from the same domain name, for example, you can go in and block that particular domain from sending you mail, regardless of how many fake addresses they make.

TURN ON FILTERS

Many services let you review suspected spam messages and confirm or deny if you want them, thereby improving the artificial intelligence that determines what goes in your inbox.

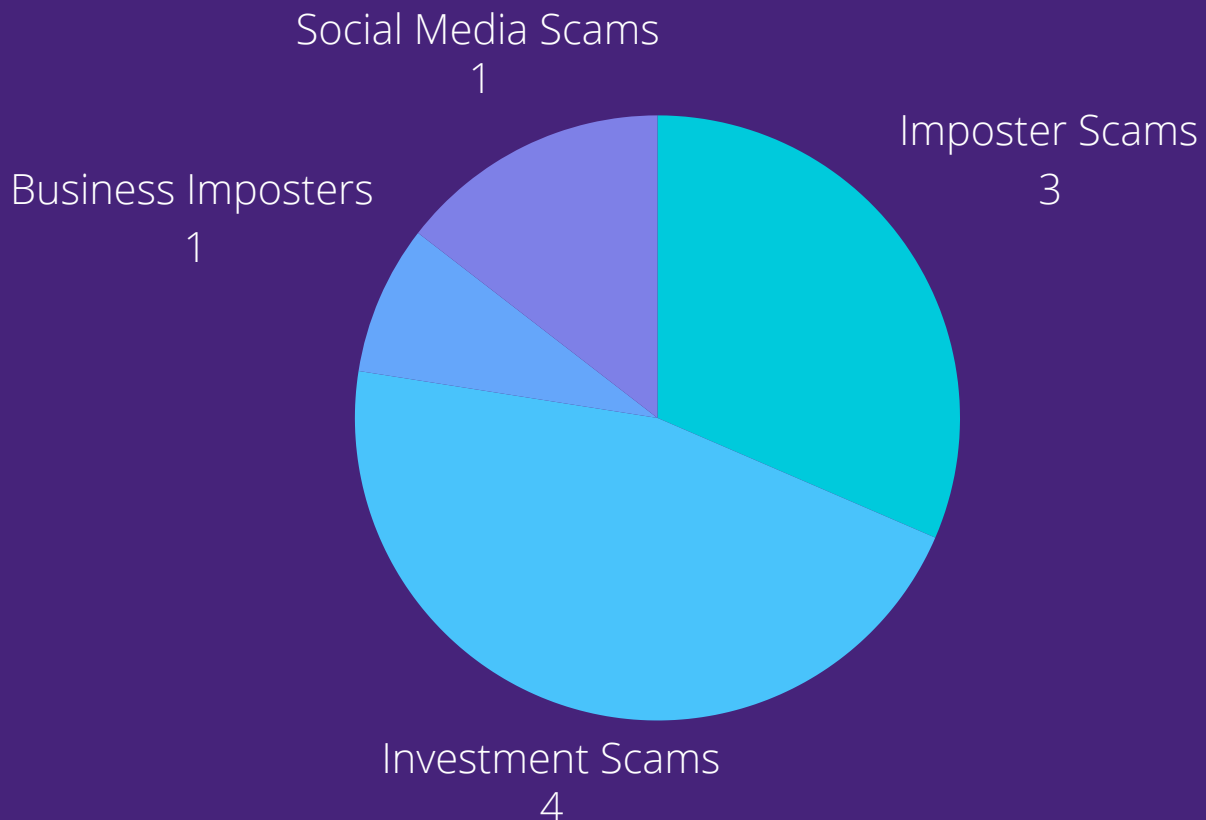
CHANGE YOUR SETTINGS

Set your email to only allow messages from known senders. Use this option with caution, however, because there's plenty of instances where unknown contacts reach out to you for legitimate, wanted reasons.



SPAM & SCAMS

*money lost to fraud in 2022
(total: \$8.8 Billion)*



Fraud is a serious problem and it can cost you big money! According to the FBI, phone scams (known as *vishing*, or voice phishing) yielded an average loss of \$1,400 per person in 2022.

Phishing and other social engineering scams have only gotten more dangerous! Know the signs and your incident response plan BEFORE something serious happens, so you don't end up part of this statistic!

TURN OFF DEFAULTS

Whenever we open a new phone, laptop, tablet or any other device, you can usually find a few applications and settings already installed on the device. These *defaults* come with the machine.

Programs that come preloaded might include...

- Web filters
- An internet browser
- Messaging features
- Calendar app
- Alarms and timers
- Backup and storage
- Digital wallets
- News
- Email apps

Some of these you might use and prefer. Others, not so much.

Experts recommend that you actually ***delete apps that you don't use.***

Not only will this help your run faster, since it's not burdened with so much memory and storage, but this will make your devices safer.

If you're not using some programs, then toss them! Hackers LOVE exploiting known vulnerabilities in outdated apps.

Not only will deleting useless default applications make your computer run faster and clear up clutter, but it will actually keep you more cyber-secure, too!

CHANGE PRIVACY SETTINGS ASAP

We can't always help what information websites require when we sign up. Often, just creating an account means giving away our names, emails, and sometimes phone numbers and other private info too.

Change your privacy settings to hide your email, number and address.

Displaying this information only gives cybercriminals more chances to get to know confidential info that they have no right to see.

Create privacy groups like Friends and Close Friends versus people you don't follow, and give them access to certain levels of information ONLY if you know them in real life.

If you do choose to give away your contact information, make sure you KNOW who's behind the screen and do so on a secure, private chat.

Yes...it's really that important!



Phishing continues to be one of the most prevalent threats to our private information. Something as simple as changing the default options on your profiles will make it harder for digital stalkers to create targeted **spear-phishing** campaigns just for you.

Unlike traditional phishing attacks, which are typically sent to a large number of random recipients, spear phishing attacks are carefully crafted to appear legitimate and trustworthy to their intended victims.

When your About Me page is completely filled out and your privacy settings are at default, it can be VERY easy to learn enough about you to concoct a convincing scheme.

So...who can view your profile? Can anyone reach out to chat directly, or just approved friends? Do you even know everyone that you follow? Taking one minute to change your privacy settings can make a huge difference for your safety!

WHAT CAN YOU DO TO STAY SECURE?

1

Be suspicious of any unexpected messages, especially those that ask for sensitive information or contain urgent requests.

2

Always verify the sender's email address or phone number before clicking on any links or opening attachments.

3

Pay attention to any inconsistencies in the message, such as typos, grammatical errors, or unfamiliar formatting.

4

Hover over links before clicking to see the actual destination URL. Do not click on links if you are unsure of their legitimacy.

5

Create strong and unique passwords for all of your online accounts, using at least 12 letters, numbers and symbols.

6

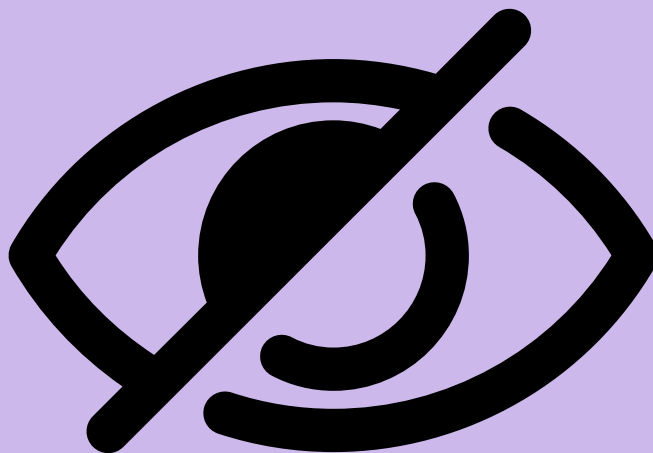
Make sure your operating system, web browser, and other software are up to date with the latest security patches.

7

Use reputable anti-virus and anti-malware software to protect your device from malware infections.

"Privacy is not something that I'm merely entitled to,
it's an absolute prerequisite."

- *Marlon Brando*



REAL REVIEWS. REAL SATISFACTION!

Art Graham

I needed a supplier that could respond quickly. BizCom has been the most responsive partner we have. Our ability to react quickly to customer needs has improved tenfold.

Partner, StellaMSP

John Gatti

As we were working on a project with BizCom, something unexpected came up that significantly delayed the project. Through the whole process, they were very understanding and accommodating. I am impressed with how much they worked with us to work around this issue.

*IT Director, Durham
Rescue Mission*

CYBERSECURITY YOU CAN TRUST!



We believe in providing YOU the best-in-class security suite to keep you cyber-secure in the face of the ever-changing threat landscape.

Call us today at **919-855-8399** and let us help you wrap a security blanket around your business.



MANAGED CLOUD, IT & CYBERSECURITY