Weekly Habits For A Cyber Secure Year

52 Weeks of Cybersecurity Tips

52 Cybersecurity Habits

Good **habits** for a cyber-secure life

It's never too late to start developing good habits. That's why becoming more cyber secure should not be a New Year's resolution but an ongoing project that you can start anytime you want. Becoming cyber secure in your day-to-day life is not a one-time thing. It's a series of habits-the things we do and don't do without thinking about them-and a healthy dose of awareness. It's knowing the risks and behaving as if those risks apply to you, because they do. We should all stand together and do our best to minimize the sucess of cybercriminals. Let's start small and gradually build up new habits from week to week. Use this guide to get you started, add one new habit a week, and pretty soon you will be cyber secure without even having to think about it.

Best of luck,
The GLS Team

Start Now

Be aware of phishing

We'll start our habit-forming journey off by becoming very aware of phishing. 90% of all successful cyber attacks can be traced back to phishing. That means that if people stop falling for phishing, we could really minimize the risk of successful cyber attacks. Who wouldn't want to be a part of that solution?

Week #1

Be extra careful about attachments in emails

Phishing emails have either fake links or malicious attachments. If you get an email from an unknown sender with an attachment, it could be malware. You should also think twice before opening attachments from known senders, especially if you weren't expecting them. Call them before opening the attachment and ask what it is.

Week #2

Hover over links in emails

Fake links come in many forms. Sometimes they look like legitimate web URLs, but when you hover over them with your mouse another URL is displayed. So even if a link in an email claims it will take you to www.amazon.com, hovering over it might reveal another URL, which is where you're really going. Sometimes web URLs or even the sender's email address have tiny errors in them. It could be amaz0n.com or even amason.com - simply to trick you into trusting that the email is legitimate and that you have nothing to worry about.

Week #3

Don't respond to threats in emails

Any legitimate service you use would never send you an email threatening to close your account with only a few hours' notice. Scaring people into action is a hacking method and it unfortunately works. Even if an email sounds threatening and calls for immediate action, take a little time to think. Remember the first two habits? If you believe an urgent-sounding email to be legit, type in the correct website URL in your browser and access your account from there. Never follow links in these emails.

Week #4

Remember that phishing can be done without emails

Maybe you thought that emails were the only phishing method hackers use, but unfortunately that's not the case. They can use instant messaging, social media posts, and even phone calls (also known as Vishing or Voice Phishing) to try and scam you for your personal information. Be careful about who you give your sensitive information to.

Week #5

Double check email addresses

When someone sends you an email, their email address is visible to you. However, hackers can disguise their email address and make their emails look like they come from someone else. They can also create email addresses that look very similar to the one they're spoofing the only difference being a little typo. You can hover over or click the sender's email address to find out if the message is coming from the right source. Read it carefully to see if there is a typo.

Did you know...

Healthcare is the number one targeted industry by hackers. More than 93% of healthcar organizations have experienced a data breach over the past three years, and 57% have suffered more than five data breaches during the same timeframe.

Keep sensitive data safe

Sensitive and confidential data can be worth a lot of money to the wrong people. Willingly or accidentally leaking data about your workplace or its clients can have sever consequences. it can even result in hefty fines.

Week #6

Keep a clean desk

If you work with confidential data, anyone walking past your desk could use their smartphone to record or photograph private information. Keep the data safe by locking it up while not in use. Bonus: Your desk will look better.

Week #7

Keep confidential documents safe at all times

Documents and data might be safe enough inside your workplace, but once you take them out of the office they could be at risk. Keeping them safe means encrypting any drives they are on and never leaving physical copies unsupervised. For instance, leaving unencrypted drives or printouts in a locked car is not a good idea.

Week #8

Don't forward confidential files to your personal email account

It's tempting to move documents to a personal device to be able to work on them from anywhere, but doing so increases the risk of a data breach. Your personal email is not as secure as your work email. The same goes for personal cloud storage. In most cases. these third-party devices and services do not comply with security policies, and using them could be interpreted as theft of company data. If you need to work on data outside your workplace, check your security policy first for directions.

Week #9

Report data leaks if you become aware of them

If you become aware that a data leak has occurred, even if it was accidental or wasn't your fault, report it. Quick and honest reporting of a data leak is always better than having it discovered later (or by the authorities). Make it this week's mission to find out what your workplace's policy is regarding data leaks and how to report them.

Protect passwords

Our lives are getting bigger online. We do almost everything in the online world, from emailing to banking and shopping. Because of this, there is a lot of information about us floating around on the internet that we need to protect. Once of the ways we do that is by using a password for our online accounts. This means that passwords are a valuable commodity to hackers. If they het ahold of your passwords, they can get into your online accounts and do a lot of harm.

Week #10

Keep your passwords safe and strong

Strong, un-guessable passwords are the name of the game; the more complex, the harder they are to guess. But unfortunately, strong and complex passwords are also hard to remember. To make it easier for you but harder for the hackers, create your passwords by combining many short words that are easy for you to remember, using a full sentence, or creating acronyms from sentences. Just don't use famous sentences or quotes.

Example of a combination of words:
CoffeeBeerWine2934

Example of a full sentence:
KiwiNeedsAnInvoiceForAPen2891

Example of an acronym:
knAifAp2891

Week #11

Use different passwords for different accounts

One of the habits that could save you a lot of grief is to use different passwords for different accounts. That means that the password you use for your social media, e-commerce accounts, smartphone, and banking should not be the same. If hackers manage to breach any of the sites you log into, they will try your password for that site everywhere. Their success rate will be considerably lower if you haven't used the same password anywhere else.

Week #12

Don't write down your passwords

Passwords can be hard to remember, but writing them down and storing them near your computer is like taping your key to your front door....very handy for hackers. Remember the first habit for creating strong passwords?

Week #13

Check your surroundings before typing in your password

Hackers don't always guess or hack passwords. Sometimes they literally just watch you type it in. All it takes is a glance over your shoulder. Because most people have access to cameras in their smartphones, they could also record you discreetly while you're logging into a private account. Avoid typing in your password in public or look for an area where your back is against a wall.

Week #14

Use multi-factor authentication

To increase the safety of your online accounts, make sure you enable multi-factor authentication (also known as 2-factor authentication). When you add an extra layer of security around your online accounts, it makes them that much harder to breach-even if hackers somehow get ahold of your password. Multi-factor or 2-factor authentication can be a one-time password sent to your phone, a fingerprint or retina scan. or a security question that only you know the answer to.

Up your online security

A lot of small habits will improve your general online security. The next few weeks will focus on the little things we need to be aware of to stay secure in our day-to-day lives.

Week #15

Treat your work email address like it's sacred

You should never give out your work email address for personal matters. Keep a separate account for your personal correspondence. This minimalizes the risk of phishing email getting into your work inbox, and therefore minimizes the risk of a data breach. Only use your work email address for work-related matters. It's also helpful to remember that the less you give out your email address, the less spam you'll get.

Week #16

Be careful when using free open WiFi

Free open WiFi connections are convenient when you're on the go or traveling, but they're also unsafe. Hackers can position themselves between you and the connection post, which allows them to gather passwords and other unencrypted data. If you need to work on sensitive documents online or log into personal accounts, it's safer to use your private data plan.

Hackers can also use public WiFi to distribute malware. If you allow file sharing on your computer, it is quite easy for a hacker to plant infected software.

Week #17

Don't connect unknown USB drives to your computer

Dropping infected USB drives on the ground around offices is a popular method hackers use to gain access to data or accounts. They leave these USB drives lying around in the hope that unaware people might pick them up and connect them to their computer. Once connected, the USB drives upload malware or spyware onto the computer, which can then infect the whole office network. Hackers can then steal sensitive data or destroy important files. A good rule o thumb is to never connect a USB drive to your computer unless you bought it yourself from a legitimate source or if it was issued to you by your workplace.

If you do find a seemingly lost USB drive, pick it up and give it to the IT department.

Week #18

Be careful what you share online

From the name of your childhood pet or favorite teacher to your hobbies and interests, hacker love to find out as much about you as they can. They can use this information to guess your passwords or tailor their phishing emails especially to you-which increases the likelihood that you'll click a link or open an attachment.

Be careful what you share about yourself online-both on social media and open forums-so that hackers can't target you.

Up your physical security

Hackers don't just lurk online. Sometimes they seek to gain physical access to your workplace or your house, where they can position devices, copy or steal files, or destroy equipment. For this reason, security is not just about what you do on your computer or smartphone but also about what you do when you're offline.

Week #19

Make sure no one follows you through access control

Just like you wouldn't let a stranger follow you into your house, you shouldn't let a stranger into your workplace. If you work at a big office it can be hard to know who is supposed to be there and who isn't, but if there is some form of access control you should be careful not to let anyone follow you through. Don't think that a stranger hanging around your workplace is someone else's problem or that it's rude to ask them who they are and what they are doing. If they're not accompanied by a member of staff they could be a threat. Everyone is responsible for keeping the workplace safe.

Week #20

Think twice before you help out

The desire to help others is a good instinct. Unfortunately, there are people that are more than willing to exploit that. They will try to get access to restricted areas using various tactics that trigger your sense of helpfulness. For instance, they could be carrying heavy boxes and pretend they can't open a door because of it. They could also be disguised as a delivery person or someone doing maintenance. Keep in mind that no one should be unaccompanied within your workplace for any reason.

Week #21

Check your computer ports regularly

Have you ever looked at the wires and ports on the back of your computer? Do you know what they're supposed to look like? If a hacker has gained access to your office they might have added a device to your computer that monitors what you do. It could look like a small USB drive or some kind of adapter that connects your keyboard to your computer.

If you find an unknown device connected to your computer, let your IT department know immediately, Removing the device might not be enough as it might have infected your computer with malware.

Week #22

Make sure to check your surroundings before giving presentations

When presenting information-especially sensitive or valuable information-during meetings, you should always be aware of your surroundings. Whether you are on the ground floor where people are walking past, or on upper floors where people in neighboring buildings might have a clear view of your presentation screen, make sure the information is safe from prying eyes. Also, make sure that visitors coming into your workplace can't accidentally see information that isn't meant for them.

Did you know...

Companies in all sectors face massive expenses due to data breaches. The average cost of a single data breach is around $3.86 million USD. This factors in loss of clients, and the serious hit to reputation. With GDPR and other privacy laws now in effect, companies may end up paying huge fines for a data breach. It is estimated that the total cost of data breaches each year is a whopping $3 trillion and will surpass $5 trillion by 2024 due to increasing fines.

Be more careful online

Most internet users are aware that it's not the safest place and that we should be careful what we interact with. Unfortunately, why it's so important to be suspicious of anything you find online.

Week #23

Close pop-ups immediately

Numerous businesses use pop-ups to tell you about interesting offers when you enter their site. These are easily closed and typically harmless. It's the pop-ups that require you to take any kind of action that you should be wary of. Sometimes scammers use pop-ups to trick you into installing software or that could take you to an infected site if you click on anything other than the "X" button (even the "Cancel" button isn't safe). If any one of your favorite websites has been breached, they could show you a pop-up that you might be inclined to trust and click on.

Week #24

Check for HTTPS in the beginning of URLs

A website that starts with HTTPS is the secure version of HTTP. HTTPS stands for Hyper Text Transfer Protocol Secure. The protocol encrypts the data sent between your browser and the website. If a hacker managed to break into the connection, they would not be able to decrypt the data. This is especially important if you're using an unsafe network, such as free WiFi.

Before you type any information on a website, make sure you see either HTTPS or a lock sign in the beginning of the URL.

Week #25

Don't accept downloads from websites

Even trusted websites that we visit can often become pawns in a bigger game for hackers. Breached websites can be used to trick people into downloading malware or ransomware. Software updates and downloads offered by a website - any website - should not be trusted.

Did you know...

The financial sector is one of the most sought after targets for hackers, but it is also the best protected. They have good reason to protect themselves: the cost of cyberattacks is the highest amongst financial institutions, reaching $18.3 million annually per company. 70% of financial companies experienced a security incident in 2018. According to recent data, they have reported a significant increase in cyberattacks due to the Covid-19 pandemic and the switch to a remote workforce.

Enable those security features

Almost all of our connected equipment has security features that we have to enable. Sometimes we are so excited to start using the equipment that we fail to give these features our attention....and then we forget. What happens next is anyone's guess.

Week #26

Lock the phone

Our smartphones are small and powerful computers. They often hold valuable confidential information and have access to online accounts that we wouldn't want to fall into the wrong hands. Locking our phone is a simple way to protect it. Our phone should always be locked when not in use.

Week #27

Update the apps on your smartphone

For the same reason that you perform regular updates on your computer, you should also update the apps on your smartphone and other smart devices as soon as they become available. Removing apps that you don't use us also a good idea.

Week #28

Don't leave your computer unlocked and unattended

This is important both at home and at the office. Leaving your computer unlocked and unattended can cause serious security problems. Anyone who has access to it, whether that's hackers, spouses, or children, could cause damage or a data leak. You could also be held accountable if someone impersonates you online. Always lock your computer when you step away from it.

Week #29

Secure the home WiFi

Home networks are often set up in a rush. If the security features on the router are not enabled, the home network could easily be accessed by hackers. Routers have their own operating systems, software and vulnerabilities and sometimes they advertise their type and make in the wireless network name. This makes it easier for hackers to gain access and get onto your home WiFi. The router's firmware should also be updated on a regular basis.

Week #30

Update your computer's software

When presenting information-especially sensitive or valuable information-during meetings, you should always be aware of your surroundings. Whether you are on the ground floor where people are walking past, or on upper floors where people in neighboring buildings might have a clear view of your presentation screen, make sure the information is safe from prying eyes. Also, make sure that visitors coming into your workplace can't accidentally see information that isn't meant for them.

Be mindful of privacy laws

All over the world, governments and institutions have enacted strict privacy laws to protect consumers - that means you - from being exposed. Companies that aren't careful with their clients' data could get into a lot of trouble. This is why it's so important to be mindful of the privacy laws and regulations that apply to our business.

Week #31

Don't ask for/give out more information than is needed

Processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, as well as genetic and biometric data, healthcare data, or data concerning a person's sex life or sexual orientation is generally not allowed. Before you ask for or give out such data, think twice. Is it really necessary? Could it be illegal?

Week #32

Remember that each individual owns their personal information

Privacy laws state that individuals own their personal information and can set limits to what information companies store or process after the business relationship has ended. If a customer asks for their data back, it needs to be handed over and deleted from the company's servers.

Week #33

Don't choose convenience over security

Online PDF makers are convenient and easy to use, but it is very dangerous to send confidential information to a service that has not been verified as safe. Some of the user agreements of these services even state that after you upload data to their site, the data is theirs to keep. Even though it's stated that the data will be destroyed, you can never be 100% sure that it will be done. When you use these services, you are essentially handing data over to a third party.

Week #34

Protect sensitive data

When your clients trust you with their sensitive data, whether it's credit card information, health data, or other personal information, you're required to keep it as safe as possible. The best way to do that is to encrypt the information and only print it out when necessary. No matter how the information is stored, you must ensure that it will not be exposed to unauthorized persons. If confidential information is leaked, it can have serious consequences for your company in terms of fines and compensations, as well as reputational damage.

Did you know...

No company is too large or too small for cyber criminals to target. They have been seeking out small and medium businesses at an increasing rate even though larger companies are in possession of more data and more money. This is because larger companies are more likely to spend money on stronger defenses and security awareness training for employees. Smaller companies are therefore better targets. In 2019, 63% of small and medium-sized businesses experienced data breaches.

Be aware of scams

Some scams have become so well-known and widespread that they're easy to recognize: like a lottery you didn't participate in but suddenly won, or your super-rich and super-distant relative from Nigeria dying without leaving an heir (so their bank found you). The problem is that not all scams are as obvious - so we need to be on our toes at all times.

Week #35

Be careful of what you share with others

Social engineering is a method hackers use to scam people into sharing secrets about themselves to their workplace. They make an effort to cross your path and strike up a conversation. It could be an innocent chat about childhood pets, birth place or interests to try and guess your passwords. Or it could be an attempt to gain your trust and friendship, so that you let your guard down and give them other information.

Week #36

Don't install unauthorized software onto your work computer

There is a lot of cool software to be found on the internet, but keep in mind that some of it is a scam designed to infect your network. Even if the software looks like it could make your work easier or help you and your colleagues get organized, you should be wary. If you install software that is infected with malware or ransomware, you could be endangering your whole workplace. Always ask the IT department for permission before installing software onto your computer.

Week #37

Avoid online personality tests

Online personality tests are a lot of fun. Who wouldn't like to find out which Beatle they are or what their superpower would be? Just keep in mind that these tests might have been created by hackers to get their hands on your information, such as your friends list, interest, email addresses, and more - all of this is very valuable to hackers.

Week #38

Double check before you trust messages in emails

One of the scams hackers regularly run is finding business emails and using them to scam employees. They either disguise their email addresses and make them look like they're from a boss, or they infiltrate an email account to send out emails on behalf of that person. Usually these are emails that require action on your part, such as transferring money to an account or opening attachments. Whenever email message require such a transaction, you should verify them through other means, such as with a phone call or by talking face to face.

The same goes for personal emails between you and other businesses. If they require a money transfer, you should always double check before you pay.

Week #39

Don't fall for suspicious instant messages from friends

Sometimes our friends send us great things, but they could also inadvertently send us something infected with malware. This malware helps hackers take over social media accounts and use them to send out malicious links or direct messages to friends. Sudden messages from friends asking you to "Check this out!" or asking "Is that you?!" with a link attached, as well as messages claiming that they need to send a verification code your phone for a "game," are very likely phishing attempts designed to infect you too. Always double check with your friends through other means if they send you such messages, and warn them that someone may have breached their account.

Did you know...

Security threats connected to smart phones and other connected devices are on the rise. Smartphones and tablets are effectively replacing desktops for many business tasks. However, mobile devices don't always offer the same level of built-in security or control as the organization-owned desktop computers they are replacing. According to a study by IBM, users are three times more likely to facilitate a phishing attack when using a mobile device.

Be careful everywhere

Cyber security is not just about the Internet. Being cyber secure relates to almost everything we do. Because of this, it is important to always be on the watch for threats. We never know who might be listening to or watching what we do.

Week #40

Don't discuss work matters outside the workplace

It's fun hanging out with your friends from work after hours. At bars, restaurants, or other social hangouts, it might be tempting to discuss things going on at work. Just make sure that you don't discuss work matters where outside parties can hear you. Information about your workplace might be valuable to others. And yes-when talking to your co-workers at bars and restaurants, other people can hear you and will listen in.

Week #41

Handle hard copies with care

First of all, we need to be careful what we print and how we store it. Leaving hard copies in the printer is not safe, especially if it's a communal printer. Second, we need to save or dispose of all printouts properly. Confidential materials should be locked up when not in use and printouts that belong in the trash should be shredded first. Although it might not seem that sensitive at the time, if someone rummages through your trash they could discover a lot of useful information. Accumulating copies of invoices or bills from your trash could give criminals valuable data about your business and clients, along with new and inventive ways to scam you.

Week #42

Choose your apps wisely

If you're discussing something that must remain confidential be aware that apps can contain malware features that allow hackers to turn on your camera or microphone and listen in on your conversations. To be absolutely sure no one is listening, keep your phone in another room while discussing confidential matters.

As a rule of thumb. don't download apps you don't need, disable features in apps that allow access to your location, microphone, or camera, and remove apps you no longer use. A regular virus scan is also a good idea.

Week #43

Keep online meetings private

Online meetings have really saved the day. They allowed us to continue our business and keep up with our co-workers, meet clients, and see our friends and family during a difficult time. Unfortunately, this has given Internet trolls the chance to have their twisted fun by crashing meetings.

No matter what video conference software you might be using, it's important to keep the invite links as sage and private as possible, and to change them regularly. It foes without saying that meeting links should never be shared on social media or public forums. Also, make sure to enable all the security features offered by your meeting software.

Did you know...

Retailers store a magnitude of valuable data and are facing an uphill battle against data breaches. 62% of consumers are not confident about the security of their data with retailers. Of those who had been victims of fraud, 52% said that the incident negatively impacted their view of the retailer. By knowing which threats to watch out for, training employees and being proactive about addressing risks, retailers can stay ahead of the game.

Avoid common mistakes

We all make mistakes. Sometimes it's because we don't know any better, and sometimes it's because we are in a hurry. Data leaks and malware infections often happen because of clumsy mistakes that can be easily avoided if we just take a moment to consider what we are doing.

Week #44

Be careful when you hit print

If you're working at a big office and using network printers, make sure you select the right printer before you hit the print button. When printing sensitive documents, double-check that the printer you are sending them to is the one closest to you. As soon as you've hit that button, go to the printer and get your printouts so they won't reach the eyes of unauthorized people.

Week #45

Distrust the auto-fill feature of your email

Many email programs have an auto-fill feature that populates email addresses for you. However, if we're not careful, that feature can work against us. Often, confidential information is leaked because email senders are in a hurry or distracted and select the wrong recipient from the auto-fill suggestions. Before you it the "Send" button, take a second to make sure your email is going to the right people.

Week #46

Always verify information on invoices before paying them

Scammers occasionally attempt to infiltrate accounting departments with fake invoices. Sometimes, they monitor email exchanges and intervene when invoicing discussions begin. Other times, they issue invoices from non-existent companies for services never rendered. They may also impersonate real businesses, falsely claiming a change in bank details. If you receive an invoice, either through mail or email, refrain from immediate payment, particularly if there's a change in account details or if it's from an unfamiliar company. It's crucial to verify the invoice's legitimacy through a brief phone call.

Be safe when shopping online

Online shopping has become a year-long event even though most of it takes place shortly before the end of the year. This means that scammers will try to trick us year round with "awesome deals" and fake package delivery notifications. We all have online shops that we know and trust, but every year new brands announce cool products and great prices that make us want to try them out. Unfortunately, many such shops are created as a front for scammers who will use the site to steal your personal and payment information.

Week #47

Don't announce you're going on vacation

Some of us like to brag on social media and that's okay, because how else would people know what a fabulous life we're living? But blasting our travle plance so the whole world knows that we're not at home could be dangerous. Not only are we putting our private lives at risk by advetising that our houes are unoccupied; we're also alerting hackers to the fact that we're not at the office. Wait to brag about your vacation on social media until after you get home.

Week #48

Choose safer payment options

By using PayPal, Google Pay, or Apple Pay, you won't be giving your credit card number directly to the online shops you order from. This might not save you from being scammed 100% of the time but it will prevent scammers from retaining your credit card information to sell to others or to keep billing you. It's also easier to report scams and false payments through these services. Avoid paying for online purchases with your debit card or via a wire transfer.

Week #49

Always do your research

Many email programs have an If you're ordering something from a new online store or one you haven't done business with before, check their reputation first. Search for the brand name and look for reviews or recommendations before you place an order. Multiple reports of fraud should give you a hint that your money is better spent somewhere else.

Week #50

Check your credit card statement regularly

It's important to keep track of how you spend your money. If hackers get ahold of your credit card information, they will likely start using it to make purchases. They will probably keep these charges small hoping that you won't notice or that you won't be bother to report them. Regardless, of the amount, always report suspicious charges if you see them.

Week #51

Be distrustful of delivery emails

Scammers and hackers know that it is more than likely that their targets have ordered something online. So, they can create phishing emails with fake delivery information, offering you the ability to track your shipment or telling you that you must pay a small fee due to a miscalculation. Instead of clicking the links in these emails, go to your browser and type in the correct URL for the shop or shipping service you're doing business with to find this information.

Week #52

Avoid offers that are too good to be true

If an offer sounds too good to be true, chances are that it is. Be wary of offers that are pushed through social media ads from unknown businesses. They will often carry a tone of urgency, claiming that they're almost out of stock or that the shop is going out of business.

Be a cyber security awareness advocate

Security is everyone's responsibility. Don't wait for the IT or training department to get involved. Be an advocate for cybersecurity awareness in your organization. Practice good cyber hygiene and encourage your peers to do the same. Each step we take to be more secure not only protects our organization, but also helps us to protect our personal information as well.

Connect with Global Learning Systems on social media:

Strengthen your human firewall.

www.globallearningsystems.com