The Driz Group

52 Cybersecurity Tips for Personal or Business Application You Need in 2022

Here are 52 cybersecurity tips that you can apply to improve your online safety whether you're using the Internet for personal or business purpose.

www.drizgroup.com

Table of Contents

Cybersecurity Tip #1: Cyberattack isn’t a matter of if, but when

Yes, there are people and businesses who have deeper pockets than you or have more interesting data than you. This doesn’t mean cybercriminals don’t find you attractive.

Most of cyberattacks aren’t targeted for the rich and famous. Cybercriminals simply automate their attacks and victims are hit not by how deep their pockets or how famous they are but by how weak their cyber defenses are. Don’t be an easy target.

Cybersecurity Tip #2: Malware 101

Malware comes from the words malicious and software. A malicious software is one that’s maliciously injected by cyber criminals into your desktop, laptop, smartphone, tablet or internet of things (IoT) devices like wi-fi router, CCTV camera or smart TV.

Cyber criminals have found and are continuously finding creative means to deliver malware into computers using website, ads, and email to name a few, causing damage to the devices, stealing data, and committing other cybercrimes.

Cybersecurity Tip #3: Don’t trust public charging stations

You’re long away from home or from the office and your smartphone’s battery is about to die. You spot a public charging station.

Hold up, public charging stations are ripe places for the cyberattack called “juice jacking” – a form of cyberattack that compromises public charging stations, stealing all the data on a smartphone that connects to it or installing a malware into the smartphone.

Charge your phone before you go out or get your own portable charger, also known as a power bank.

Cybersecurity Tip #4: Use 2-Factor Authentication

Who can blame you if you use the name of your dog as your password or use the monumental 12356789 password? There are just too many passwords to remember, from email accounts, bank accounts to your Netflix account.

While it isn’t advisable to use easily hacked passwords like 12356789, it’s best to use 2-factor authentication for your sensitive accounts like your primary emails.

The 2-factor authentication ensures that you're the only person who can access your account, even if someone knows your password. It will add a second step to your login process sending a verification code to your mobile that hackers won't have access to. It's easy to setup with virtually every online service.

Cybersecurity Tip #5: Never use a public computer to input your private data

In public spaces like airports and hotels, public computers are offered to guests to use free of charge.

While these public computers are beneficial to search for something, these public computers shouldn't be used, for instance, to shop online where you've to input your private data or even check personal or work email.

The public computer that you're using can be tampered with a keylogger – a malware that records every keystroke made by a computer user. Your passwords and other confidential information can be accessed this way and then used by cybercriminals to steal your information and your identity.

Cybersecurity Tip #6: Use an antivirus or a complete endpoint protection software

An antivirus won't protect you from all malware in this world but it's a cyber defense that you should have to improve your online safety. A complete endpoint protection on the other hand will provide a better protection against most online threats.

There are many options to choose from and since it's a commodity, annual subscription prices are generally very affordable.

Cybersecurity Tip #7: Delete old, unnecessary apps

Similar to cleaning out your closet regularly, same thing has to be done with your laptop, smartphone and tablet apps.

Old apps, especially those that are unsupported – software that's no longer updated by the software maker – make your devices vulnerable to cyberattacks.

Cybercriminals are particularly making malware that attacks old and unsupported software and apps to steal your personal information and evade your privacy.

Cybersecurity Tip #8: Keep all your software up-to-date

If there's an available update for any of your software, install the update as soon as possible! A software update means that the software vendor found security vulnerability in the software and provides a patch – piece of software code that fixes the security vulnerability.

The security update may interrupt your normal usage of your device, but this is a small price to pay compared to being a victim of a cyberattack as a result of failing timely to update your software.

Cybersecurity Tip #9: Stay away from websites without "HTTPS"

What does "HTTPS" even mean?

A website address that starts with "https" is a sign that whatever you input in the website is encrypted – a process that jumbles the data (for instance, credit card details) that you've input in the website into some incoherent form so that this data can't be read by cybercriminals when data travels online.

Cybersecurity Tip #10: Don't overshare

Your social media accounts are filled with photos of your furry family member. There's no harm in sharing these photos.

Don't overshare the details of your other family members like full names or dates of birth. Any of this data could be the secret answer in resetting your online account passwords without your knowledge.

Cybersecurity Tip #11: Protect your primary emails as if your life depended on them

Your online existence depends on your primary emails. Your online bank accounts are attached to your primary emails.

When your primary emails are compromised, this could lead to the compromise of your other important online accounts. So, protect them as if your life depended on them (really). Protect them with strong passwords that are not based on a dictionary words and use 2-factor authentication. Remember, "Linda123" is a weak password that could and will be easily guessed by cybercriminals.

Cybersecurity Tip #12: Free your primary emails from spam emails

Similar to the origin of the word “spam” – canned meat that clogs your arteries, spam emails are similarly harmful to your online health or security.

A spam email is an unsolicited email, a copy of which is sent to hundreds of thousands, if not, millions of recipients. Majority of malware – malicious software - is delivered through spam emails.

Never open an unsolicited email even when the subject line is catches your attention. Delete it automatically.

Cybersecurity Tip #13: Watch out for fake ads

Who can resist a 70% off sale? Not many. But if this is an online advertisement, be wary of it. Cybercriminals are getting their hands on what appears to be legitimate online advertisements but are, in fact, fake ones.

Known as malvertisement, from the words malware and advertisement, these fake ads install malware on your device once you click on it.

Use an adblocker to protect your devices from malvertisements.

Cybersecurity Tip #14: Download an app from official sources

Want to learn a new language? There’s an app for that. Almost everything nowadays has an app.

Only download an app from the official website or from official app stores including Apple and Google.

Cybersecurity Tip #15: Scan apps for malware

Not all apps from official app stores, Apple or Google, are free from malware. While these official app stores make it a point to screen out apps with malware, some malicious apps aren’t screened out.

Use an antivirus or endpoint protection software that screens apps prior to installing into your device.

Cybersecurity Tip #16: Fish out phishing emails

A phishing email is an email that looks like it comes from a trusted source, but it isn't. Cybercriminals use phishing emails to gain your trust for you to reveal sensitive data or convince you to do something.

For instance, you may receive an email that looks like it comes from your bank, asking you to reveal your account login details. A close scrutiny though reveals that the email address of your bank is slightly modified to fool you into thinking that it's a legitimate email from your bank.

Never throw away caution whenever an email asks for your sensitive data. Remember that login details are your personal information. Your bank will never ask for your login details via email or over the phone.

Cybersecurity Tip #17: Monitor your email activity log

If you've a Google email account, you can monitor who have access to it – what browsers, devices, IP addresses they are using and when they accessed it.

You can terminate unwanted access to your email account with a single click.

Cybersecurity Tip #18: Be careful what you click

Something pops-up in your computer screen: a box where there's a "Download Now" button to download the latest version of Adobe Flash.

But you don't even know what an Adobe Flash is. Never click on pop-ups like this. Cybercriminals lure victims to click on pop-ups like this in order to install malicious software on your computer that would allow them to use it against other computer users like you.

Cybersecurity Tip #19: Put a tape over your laptop's camera

Mark Zuckerberg does it, so should you – put a tape over your laptop's camera, that is.

A malicious software can turn your laptop, smartphone, or tablet camera into a spy camera. Better be safe than sorry by putting a tape over that camera.

Cybersecurity Tip #20: Have more than one email account

Never rely on one email account. Create different emails for different purposes.
For instance, the email account that links to your Netflix account should not be the same as the email account you use for your bank account.

Cybersecurity Tip #21: Never trust an email attachment, even from a friend

You’ve just received an email from a friend with the subject line "ILOVEYOU". You’ve scrutinized the email address and indeed it’s from a friend – one that you’re fond of.

Your friend’s email says, "kindly check the attached LOVELETTER coming from me." Should you open the attachment?

In 2000, millions of email recipients opened an email with the subject line "ILOVEYOU" and downloaded the attachment assuming that it was a love letter. What was downloaded was, in fact, a malware that wiped out all computer files.

So, even if the email address appears to be from a friend, never open an attachment. An email address nowadays can be spoofed.

To be safe, directly contact your friend to verify if he or she indeed sent the email. Don’t use the Reply button. Create a new email using the email address that you’ve saved in your contacts.

Cybersecurity Tip #22: Don’t forget to do a factory data reset

Feeling generous or running out of cash? Your laptops, smartphones and tablets are valuable products to giveaway or earn cash.

Before selling or giving them away, don’t forget to do a factory data reset or even “sterilize” your device using specialized tools. This will delete all your personal data like email details, sites that you’ve visited and photos and videos that you’ve taken.

Cybersecurity Tip #23: Stay away from USBs and external hard drives

Anything that’s plugged into your laptop like USBs and external hard drives is a potential source of malicious software.

As such, stay away from them or find excuses not to use them, especially if they come from untrusted source. If you must use them, first disable the auto-run option and use an antivirus to scan the content.

Never plugin any USB thumb-drives that you find on the street, at the mall or at the airport. Cyber criminals use this clever technique to infect your computer with malware.

Cybersecurity Tip #24: Avoid public wi-fi

Almost all coffee shops and retail locations nowadays have public Wi-Fi. Know that whatever you access online by using a public Wi-Fi can be read or tracked by others.

You can better protect yourself buy using an inexpensive VPN service or ask your company's IT for a recommendation when away from the office.

Cybersecurity Tip #25: Use a burner phone if you want to be reckless online

If you want to visit sites that are notoriously unsafe, or you want to download an app that you're not sure it's safe, then a burner phone is a must.

A burner phone should be a separate phone. Your primary phone is one that you use for sensitive information like your primary emails and bank accounts.

With your burner phone, no sensitive data should be entered. As no sensitive data is at stake, you can do whatever you want on this phone.

Cybersecurity Tip #26: Slow performance of a device is a sign of a cyberattack

Ever wondered why your laptop, smartphone or tablet is running slow? This could be a sign that your device is has been hacked and/or tempered with.

Slow performance is one of the signs that a device is infected with a malicious software.

Cybersecurity Tip #27: Watch your back from disgruntled employees

Some people can’t seem to move on. This is the case mostly by fired employees.
Make sure that before firing someone, his or her access to your organization’s data must first be disabled.

Cybersecurity Tip #28: Never re-used a password

The name of your dog as a password for all your online accounts isn’t advisable.

Cybercriminals have long discovered that people re-used their passwords. Stolen passwords are sold in the online black market as these are used to access other online accounts.

Cybersecurity Tip #29: Use a separate credit or debit card for online shopping

Trust no one online. This should be the case every time you shop online. The risk of cyberattack on your most trusted online store can’t be dismissed.

Don’t give cyber criminals the opportunity to access your hard-earned money. Get a separate credit or debit card solely for online shopping use. Only put in the amount that you’ll use and only leave the required minimum balance.

Cybersecurity Tip #30: Never turn on out of office or vacation reply

Excited about your upcoming tropical vacation? Don’t turn on that out of office or vacation reply.

In your personal or office email, there’s an option to turn on the out of office or vacation reply. When this feature is turned on, every time people email you, they’ll receive an automatic email reply that you won’t be able to reply to them right away.

While this is mindful to legitimate email senders, this is a security risk. Criminals may take your absence as an opportunity to attack your office or your home. Fortunately, some email providers allow restricting the out of office replies to your contacts only.

Cybersecurity Tip #31: Never reveal your real location

It’s tempting to post on social media those lovely vacations photos immediately right after they’re taken or to go live via Facebook to share the beautiful scenery where you’re vacationing.

Revealing your exact whereabouts via social media postings is a cybersecurity risk. Criminals may take advantage of your absence and may do something sinister in your office or home.

The delayed postings of your vacation photos and videos will bring the same reaction from your frenemies. They’ll either love or hate you more.

Cybersecurity Tip #32: Turn off your geo-location

Turning on geo-location in your Google, Facebook, Instagram, and other social media accounts can tip criminals of your exact whereabouts.

Always turn this off to protect your privacy.

Cybersecurity Tip #33: Never use the following abused passwords

A Google and UC study revealed that passwords listed below are the most commonly used and abused passwords:

- 123456
- password
- 123456789
- abc123
- password1
- homelesspa
- 111111
- qwerty
- 12345678
- 1234567

Cybersecurity Tip #34: Mind your IoT devices

IoT devices like your wi-fi router, CCTV camera and smart TV are computers too. Protect them like your other devices such as laptops and smartphones as IoT devices are similarly targeted by cybercriminals.

Your insecure IoT device can be used by cybercriminals to form a botnet – a group of insecure IoT devices that are infected with malware and controlled by a cybercriminal or a group of cybercriminals to conduct cybercrimes such as spreading spam emails.

Changing the default passwords to stronger passwords and keeping the software of your IoT devices up-to-date are two of the best cybersecurity practices to protect your IoT devices from cyber criminals.

Cybersecurity Tip #35: Cybercriminals may be making money out of using your computers

Your desktop, laptop, smartphone, tablet and IoT are money-making machines for cybercriminals who are engaged in the cyberattack called cryptocurrency mining.

A number of cryptocurrencies, including Bitcoin, need to be mined. Cryptocurrency mining refers to the process by which transactions are verified and also a means of releasing a new digital coin.

In the past, ordinary computers were used to mine Bitcoin. Today, to mine Bitcoin, one needs a specialized and powerful computer. Other cryptocurrencies like Monero, however, can be mined using ordinary computers and even small devices such as smartphones and IoT devices.

The computational power of your devices may be small but when they are combined with thousands, if not, millions of other devices, the resulting computing power is enormous. According to a security company Avast, more than 15,000 IoT devices would be needed to mine $1,000-worth of Monero coins in just 4 days.

The thing about cryptocurrency mining attack is that this is done without the knowledge of the IoT device owner. High energy bills, poor device performance and a shortened device lifespan are signs that your IoT devices are used by cybercriminals for cryptocurrency mining.

Using strong passwords and keeping the software of your IoT devices up-to-date are 2 of the effective means to protect your devices from cryptocurrency mining.

Cybersecurity Tip #36: Your IoT devices can be used for DDoS attack

In a distributed denial-of-service (DDoS) attack, an attacker may take advantage of the weak security of your IoT device like your CCTV camera, inject a malicious software into it, control it and send huge amounts of data to a website, making a website unusually slow or making it inaccessible to visitors.

Protect your IoT devices from being used for DDoS attacks by changing the default password to a stronger one and keep the IoT's software up-to-date.

Cybersecurity Tip #37: Backup important data

Have an extra copy or copies of your important data or use a secure online storage. This way, if anything happens to your laptop, smartphone or tablet with your important data on it, you've something to fall back on.

Cybersecurity Tip #38: Prevent ransomware

Real-life crimes are mirrored online. In a ransomware attack, a cyber attacker injects a malicious software in your desktop, laptop, smartphone or tablet, encrypts all the files, locking you out of your device and asks a ransom payment from you to unlock the device.

Keeping all your software, especially your operating system, up-to-date is one of the effective means to prevent ransomware attacks. Backing up your important data ensures that ransomware attacks won't have an effect on you as you can simply ignore the ransom threat as you've another copy of the data.

Cybersecurity Tip #39: To pay or not to pay in case of a ransomware attack

If you've a backup copy of the data that ransomware criminals are holding hostage, then there's no point in paying the ransom.

Backing up your data is, therefore, very important so that ransomware criminals won't have any leverage on you.

Dilemma often comes from ransomware attack victims who haven't backed up their data. Paying the criminals, however, doesn't guarantee that you'll get your data back.

The software code of infamous WannaCry ransomware, for instance, was written in such a way that even the criminals themselves can't unlock the locked data even if the victims pay ransom.

Cybersecurity Tip #40: Install adblocker

Many online ads install malware on your computer.

To prevent malicious ads from appearing on web pages, install an adblocker – software that blocks online advertisements from appearing on web pages that you visit.

Cybersecurity Tip #41: Don’t be a victim of social engineering

Social engineering is a form of manipulation that convinces you to ignore normal security procedures.

In your personal life, you may receive a call from someone pretending to be from your bank, asking for your bank login details.

At work, you may receive a call and an email from someone pretending to be from your company’s supplier, asking you to transfer money to the supplier’s new bank account.
In both situations, you’re asked to do something that’s not within the normal security procedures. Your bank wouldn’t call you to ask for your login details. And company protocols for money transfer to a new bank account are more exhaustive than a mere phone call or simple email.

The scam at the office is what is called business email compromise (BEC) scam. It’s a form of social engineering where scammers try to convince you, especially if your work at the office is related to finance, to ignore normal office security procedures.

BEC scammers see to it that your boss is out in the office when the scam happens. Scammers will call you, email you, pretend that they represent your regular supplier and convince you to make money transfer to the new bank account of the supplier.

The scammers may send a spoof email that looks like it comes from your boss, convincing you to release money to the new bank account.

The best way to avoid being a victim of the BEC scam is to verify the authenticity of the money transfer request by talking face-to-face to your CEO or by speaking to him or her directly on the phone.

Cybersecurity Tip #42: Legitimate website may be a carrier of malware

A legitimate website doesn't mean it's a safe site. Cyber criminals are using insecure sites to spread malware through a cyberattack called drive-by attack.

The attack is called "drive-by" as this requires no action from the victim, other than visiting a website.

Criminals may plant the malware on the site visited by the victim, or the criminals may redirect the victim to another site and from there infects the computer of the visitor with a malware.

Typical victims of drive-by attacks are computers with outdated software. To prevent drive-by attacks, it's important then to keep all your software up-to-date by installing updates as soon as it becomes available.

Cybersecurity Tip #43: Delete potentially unwanted apps

Potentially unwanted apps (PUA) are software that you haven't intentionally downloaded. They're just downloaded along with an app that you intentionally downloaded.

These unwanted apps could display pop-ups, install browser extensions and even change your current browser. They may be harmless at first, but once cyber criminals get hold of them, they could become malicious overtime.

One way to prevent unwanted apps from entering your computer is by going to advanced setting whenever you download an app. In the advanced setting, uncheck the apps that you don't want to be installed on your computer. In case you've missed this advanced feature, delete these unwanted apps manually.

Cybersecurity Tip #44: Stay off-grid

Whenever you aren't using your laptop, smartphone or tablet, disconnect your device from the internet.

Whenever you notice that a cyberattack is about to happen through unwanted pop-up ads or a rogue email, disconnect your computer from the internet immediately and use your end point protection software to scan your device.

Cybersecurity Tip #45: Exercise caution when visiting notorious sites

Torrent sites (include porn sites to the list) are notorious for being hotbeds for drive-by attacks. Stay away from sites like these. If you need to visit these notorious sites, use a burner phone, one that's cheap and can easily be discarded.

Cybersecurity Tip #46: Use your laptop as standard user, not as administrator

In your operating system, in Windows 10 for instance, you've the option to run your computer as a standard user or as an administrator.

As a standard user, you can perform common daily tasks like surfing the internet, checking emails and running software programs. As an administrator, you can add, remove software and even reset the PC to factory setting.

Setting your PC to standard user ensures that you won't unintentionally add or delete software. Only set your PC to administrator mode if you need to make conscious clean-up of the existing apps on your PC. Setting your PC to standard user will also minimize the risks of malicious installation of malware into your PC.

Have a Guest account on your computer? If you really need it, make sure you use a strong account password.

Cybersecurity Tip #47: No one could address ALL cybersecurity issues

If someone tells you that he has an all-in-one fix to all cybersecurity problems, know that he's blowing smoke.

Fifty-two cybersecurity tips are particularly listed here as there are more than one solution to preventing cyberattacks and data breaches.

Cybersecurity Tip #48: Not all hackers are bad

Everyday hackers, the good ones and the bad ones are always looking for security vulnerabilities on widely used software programs.

Good hackers, also known as white hat hackers or ethical hackers, regularly test software programs for security vulnerabilities. Once a white hat hacker discovers any security vulnerability on a particular software, this is then reported directly to the software maker in order for the software maker to issue a security update fixing the newly discovered security vulnerability.

Software makers like Google, Apple and Microsoft give monetary rewards to white hat hackers for their discovery and for directly reporting the security vulnerability.

Many software companies are also employing in-house hackers to test the security vulnerabilities of their software products.

Bad hackers, also known as black hat hackers, regularly test widely-used software for security vulnerabilities. Once they discover it, they don’t report this to the software maker and instead use it for personal gains like launching cyberattacks using the newly discovered security vulnerability or selling via online black market the information or the malicious software created specifically to exploit the newly discovered security vulnerability.

Like in the real world, there are gray areas. Same thing in the world of hacking, there are gray hat hackers. They are often a mix of white and black hat hackers. Gray hat hackers often search for security vulnerabilities for widely-used software. Once they discover a vulnerability, they’ll contact the software owner, demand a payment for the discovery or for the security fix if they’ve one. If the software maker doesn’t pay up, a gray hat hacker threatens the software maker to expose the security vulnerability to the public.

Cybersecurity Tip #49: Stay away from anything that's free online

Like in real life, nothing is free. Stay away from free apps, free antivirus, free VPN (virtual private network), free Wi-Fi.

Free stuff online almost always has a caveat, that is, free service for stealing your data, for instance. Remember Facebook's data breaches? Well, after all it's a free service.
Cybersecurity Tip #50: Do your own research in choosing any software, internet service provider or any online services.

Always do your own research when it comes to choosing anything that connects your primary devices like your main laptop and main smartphone to the internet.

Your main laptop and main smartphone are devices where you access your sensitive information like your important emails, bank accounts and other important accounts.

It's, therefore, essential that you spend time choosing the most trusted, credible software, internet service provider and other online services. A simple online search will tell you whether such online service is credible or not. If you have a friend or a family member who works in cybersecurity or IT fields, always ask for their opinion.

Cybersecurity Tip #51: What to do in case of a cyberattack?

In case of a cyberattack, your immediate reaction should be to go off the grid. Immediately disconnect your computer from the internet. Then use an uninfected device, another laptop or another smartphone to change your passwords and activate 2-factor authentication of your primary emails and important accounts like bank accounts.

What to do with the attacked device? Conduct a full scan of the device and if possible, perform a factory reset.

A full scan will aid you in discovering and deleting hidden malware, while the factory reset will erase all the data, including the malware injected into your device. The problem with factory reset though is that it'll erase even your important data.

This is why it's a good practice to backup all your important files so that if anything happens you can still have access to your important data despite the failure of one device.

There are plenty of online services that will sync your data and will keep it safe in the Cloud. Check with your IT prior to installing anything on your work computer or company issues mobile device. You could be violating company's policy.

Cybersecurity Tip #52: Cybercrime is a growing business

Here are few numbers:
$16 Million-worth of ransom payment was paid by nearly 20,000 ransomware victims during a 2-year period, a study conducted by researchers from Princeton University, New York University, University of California, San Diego, Google and Chainalysis showed.

3 Billion was lost to BEC scammers from January 2015 to February 2017, according to the Federal Bureau of Investigation (FBI).