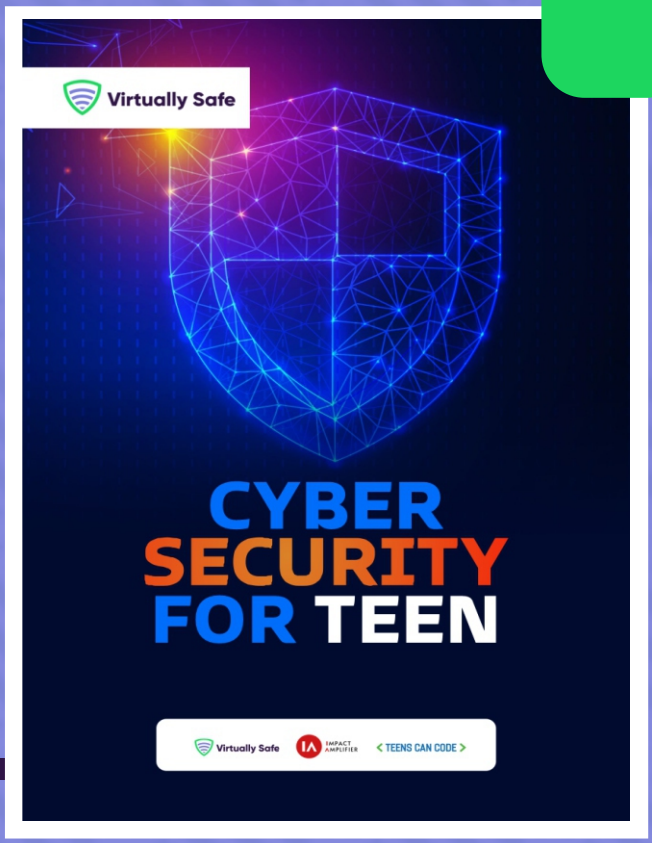
Virtually Safe

CYBER SECURITY FOR TEENS

Virtually Safe | IMPACT AMPLIFIER | < TEENS CAN CODE >



recommendations for maintaining online safety as a teenager 03

Types of weak passwords to avoid 03

What to do when you are caught in the trap 06

Cyber Security For Teens

By taking some few steps, you can protect your data on the internet and ensure the security of your digital systems.

Yes, you can effectively protect your sensitive data and computer systems by acquiring some basic knowledge, putting in a bit of effort and dedicating a few minutes of your time.

There's no need to feel overwhelmed by cybersecurity—it doesn't demand so much time or money. In fact, you can safeguard your online presence using reliable free tools and numerous cybersecurity measures can now be automated. You can even do this yourself as a preteen or teen.

If you think you need the help of your parents or a trusted adult to do so, by all means please go ahead and ask for the help. Your online security is salient.

A little amount of time devoted to getting ready can ensure your safety. Taking a few moments to gather information, prepare yourself and take necessary steps is more advantageous than the potential consequences of losing your vulnerable data in a security breach or becoming a victim of identity theft.

By adhering to our simple principles, even if some of your data is compromised, you can limit the extent of the harm.
It is important that you do this because most online criminals target young naive fellows like you and so you can't afford to stay clueless or off guard.

Below are our top 10 recommendations for maintaining online safety as a teenager:

USE LONG, DISTINCTIVE PASSWORDS

When it comes to password security, length is more important than complexity. It is important to create strong passwords that are a minimum of 12 characters long and incorporate a combination of letters, numbers and symbols. Ideally, your password should not resemble a recognizable word or phrase. Furthermore, you should have a unique password for each of your online accounts, even though it may seem challenging to remember them all.
Alternatively, you can create a password that functions as a "passphrase," which is essentially a sentence consisting of at least 12 characters. Focus on positive sentences or phrases that resonate with you and are easy to remember, like "?ILove2StaySafeOnl1ne!?" (but please don't use the above exact example).

By all means, avoid weak passwords. Speaking about weak passwords, here is what you need to know about weak passwords. First, a weak password is one that is easily guessable or susceptible to brute-force attacks.

Types Of Weak Passwords To Avoid

PERSONAL INFORMATION:
Using your name, birthdate, address, or any other easily obtainable personal information as a password is weak since it can be easily guessed or found through social engineering or online research.

COMMON WORDS OR PHRASES:
Passwords like "youandi", "oneandonly" or "mylove" are weak because they are commonly used and can be easily guessed by attackers.

KEYBOARD PATTERNS:
Passwords that follow simple keyboard patterns, such as "qwertyuiop" or "1qaz2wsx," are weak since they are easily guessable and lack complexity.

DICTIONARY WORDS:
Using common dictionary words like "sunshine" or "password" as passwords is weak because they are vulnerable to dictionary-based attacks. Never lose guard by using them.

SEQUENTIAL OR REPETITIVE CHARACTERS:
Examples of such are "abcdefg", "11223344" or "111111" are weak because they lack complexity and can be easily cracked. They are pretty common and easily guessable passwords that offer no real protection.

Strong passwords should be unique, complex and difficult to guess. It is recommended to use a combination of uppercase and lowercase letters, numbers and symbols to create strong and secure passwords.

2.UTILIZE A PASSWORD MANAGER

It's time to bid farewell to keeping your passwords in a notebook or using applications like the Notes app or word processing documents to store them. Instead, reserve those mediums for doodles or save hard drive space. The most straightforward and secure approach to managing unique passwords is by using a password manager application.

A password manager is a specialized software designed to handle all your online credentials, including usernames and passwords. Many password managers are available for free and some are integrated into web browsers and device operating systems. By utilizing a password manager, you can store your passwords in an encrypted database, envisioning it as your personal data vault. Thankfully, these programs also have the capability to generate new passwords whenever you need them.

The convenience and security provided by password managers make it easier than ever to create, store, and access your passwords. With a password manager at your disposal, you no longer have to struggle with remembering multiple complex passwords or worry about the vulnerability of using weak or repetitive passwords. Embrace the simplicity and peace of mind that comes with efficiently managing your passwords through a reliable password manager.

3. MAINTAIN A SECURE DEVICE

One crucial step in staying safe online is to prioritize the security of your internet-connected devices, including personal computers, smartphones and tablets. Keeping the software on these devices up to date plays a significant role in reducing the risk of falling victim to ransomware and malware attacks.

Regularly updating your software ensures that any known vulnerabilities or weaknesses are patched, making it harder for cybercriminals to exploit them. These updates often include security enhancements and bug fixes that strengthen the overall protection of your device. To simplify the process, you have the option to configure your devices to automatically update or to notify you whenever an update is available. This "set it and forget it" approach takes the burden off your shoulders, ensuring that you don't miss

important security updates. By keeping a clean machine and staying proactive in maintaining the latest software versions, you significantly reduce the likelihood of your devices becoming compromised and your sensitive data falling into the wrong hands. Remember, a well-maintained device is a strong defense against the evolving threats in the digital landscape.

4. UTILIZE SAFE WI-FI

Public wireless networks and hotspots lack security measures, leaving your activities on your laptop or smartphone vulnerable to prying eyes. It is advisable to restrict your actions while connected to public WiFi. Particularly, refrain from logging into important accounts such as email and financial services. To establish a more secure connection, consider using a virtual private network (VPN) or a personal/mobile hotspot.

5.NOTIFY ABOUT PHISHING

One effective method to combat cybercriminals is by informing authorities about phishing attempts, and nowadays it has become simpler than ever. In the case of receiving a phishing email on your work email address, promptly report it to your parents, or media support center. If you're working in a corporate organization, you can consider reporting to your IT manager or security team. If you're at home and the email is sent to your personal email address, refrain from clicking on any links (including the unsubscribe link) or replying to the email. Most email programs and social media platforms provide options to report phishing attempts. However, it is important to delete the phishing message without delay. Additionally, you can enhance your protection by blocking the sender through your email program, social media platform, or phone.

6. CREATE DUPLICATES

To safeguard your valuable work, music, photos, data and other digital information, you should generate copies and store them securely. By having a backup of your data, you can restore it in the event of ransomware or other cyber threats affecting your device. Likewise, if your computer breaks or crashes, you won't lose the data alongside the device. Adhere to the 3-2-1 rule when backing up your data: maintain a minimum of three (3) copies, store two (2) backup copies on different storage media and keep one (1) copy offsite. One option for storage could involve utilizing cloud backups, which involve secure computer servers accessible through an account.

7. THINK BEFORE YOU CLICK

One of the most regular and effective techniques employed by cybercriminals to gain unauthorized access to your sensitive information is through deceptive clicks. These can take various forms, such as malicious links embedded in emails, social media posts, tweets, text messages and even online advertisements. Hackers utilize these avenues as direct pathways to exploit vulnerabilities and compromise your valuable data. To protect yourself, it is crucial to exercise caution and thoughtfulness before clicking on any suspicious or unverified links or downloading unfamiliar content.

One of the primary tactics used by cybercriminals is phishing, where they create deceptive communications that appear legitimate to trick unsuspecting individuals into revealing personal information, such as passwords, credit card details, or social security numbers. These phishing attempts often rely on the urgency or curiosity of the

recipient to entice them into clicking on a malicious link or downloading an infected attachment. By falling into this trap, individuals unknowingly grant cybercriminals access to their sensitive data.
To avoid the risks associated with deceptive clicks, you should be skeptical and vigilant when you encounter unfamiliar or unexpected messages or links. Take a moment to pause and assess the legitimacy of the communication. Look out for red flags, such as poor grammar or spelling errors, suspicious email addresses, or requests for sensitive information. Remember that legitimate organizations usually don't ask for sensitive details through unsolicited emails or messages.

By counting to five or taking a brief pause before clicking, you allow yourself time to evaluate the authenticity of the communication. Pay attention to the source of the message and consider whether it aligns with your expectations or prior interactions. If in doubt, it is always better to err on the side of caution and refrain from clicking or downloading until you can verify the legitimacy of the content. You can also show the email to an experienced adult to help you verify.

Maintaining a healthy skepticism, staying informed about the latest phishing techniques and regularly updating your knowledge of online security best practices will empower you to navigate the digital landscape with confidence. By exercising caution before clicking, you fortify your defenses against cyber threats and ensure the safety of your valuable information as a teenager.

WHAT TO DO WHEN YOU'RE CAUGHT IN THE TRAP

And just in case you accidentally find yourself in a situation where you have fallen victim to deceptive clicks or are at risk due to online dangers, there are several steps you can take to mitigate the potential harm:

1.Immediately disconnect from the internet: If you suspect that your device has been compromised or your personal information is at risk, the first step is to disconnect from the internet. This can help prevent further unauthorized access to your accounts or data.

2.Change passwords: If you believe that your accounts have been compromised, it is crucial to change the passwords immediately. You should create strong and unique passwords for each account to enhance security.

3.Contact the appropriate authorities: If you have fallen victim to cybercrime, such as identity theft or online harassment, it is important to report the incident to the relevant authorities, such as the local police or a designated cybercrime reporting agency. Cyber crime is a big offense, how much more even it's carried out against a teenager like you.

4.Inform a trusted adult or guardian: You should reach out to a trusted adult, such as a parent, guardian, or teacher, to inform them about the situation. They can provide guidance, support, and assistance in taking further steps to address the issue.

5.Educate yourself about online safety: It's crucial for you to stay informed about online safety

best practices. You should learn about identifying and avoiding phishing attempts, safe browsing habits and the importance of protecting personal information.

6.Use reputable security software: Installing and regularly updating reputable antivirus and security software on your devices can help detect and prevent malicious activities

7.Be cautious of sharing personal information: As a teenager, you should be mindful of the information you share online. Avoid sharing sensitive details like full names, addresses, phone numbers, or financial information in public forums or with unknown individuals.

8. Enable multi-factor authentication (MFA): As mentioned earlier, enabling MFA adds an extra layer of security to online accounts. By activating this feature, even if an attacker has the password, they will still require additional verification to access the account.

You're not too young to self protect. Always do your part in ensuring that your personal information is safe by following the above principles.
For more information on what digital security is all about. Check out this article. link