Cybersecurity Awareness V 1.0 Defensive Measures e-book

2020 CYBERDRIP PVT(LTD) WWW.CYBERDRIP.COM VISIT NOXCYBERSECURITY.COM FOR CONSULTING

Cyber Security Awareness Program v1.0

Table of content

Social Engineering.....2

Email / IM / Bulletin Boards.....2

Web Browser.....3

Safe browser.....3

Complex passwords.....4

Social Networking.....4

Mobile Risks.....4

Encryption.....5

Data Destruction.....5

Remote working.....6

WiFi security and passwords.....6

Physical Security.....6

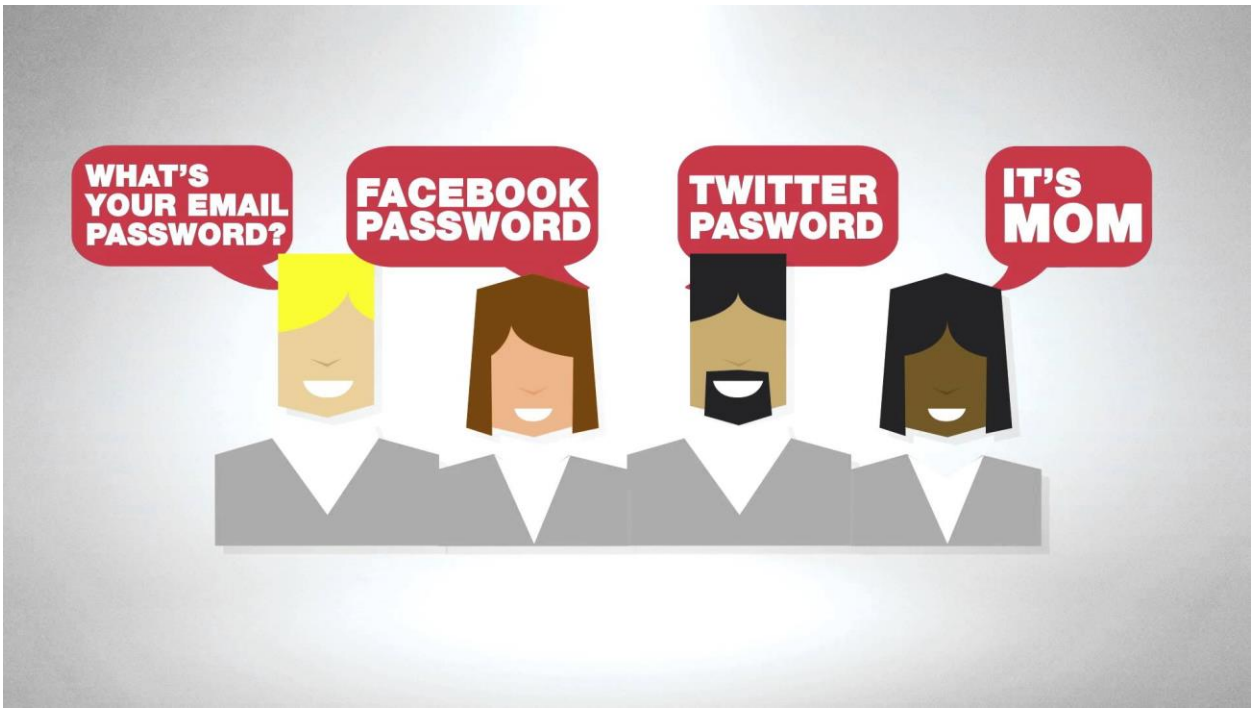
Apps permission.....7

Hacked!.....7

Subscribe https://www.cyberdrip.com/ for gamified, simplified and online training programs

Social Engineering

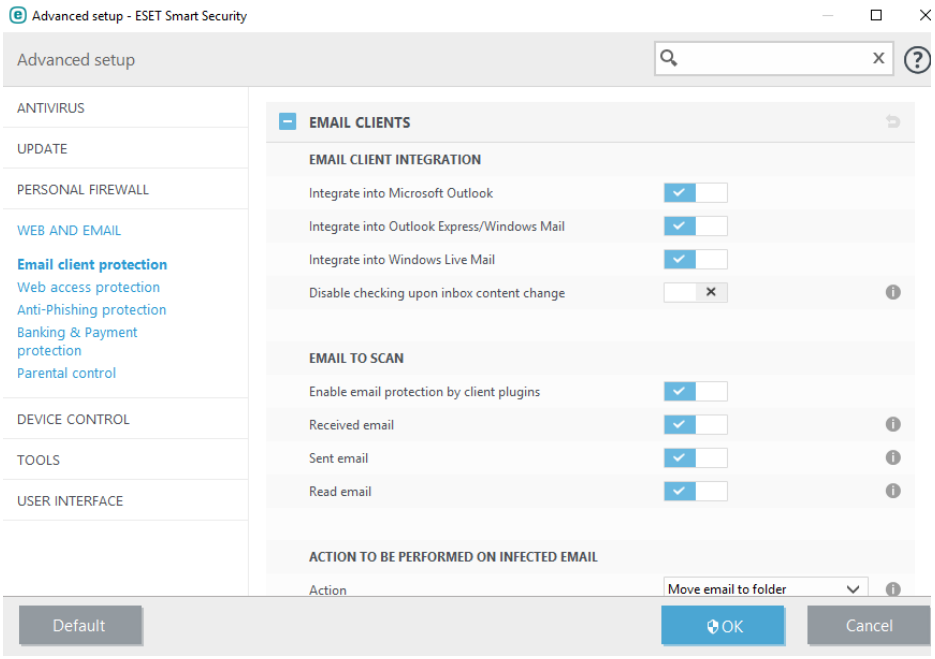
The most important thing you can do to prevent being socially engineered yourself is to always be as vigilant as you can. Never give out any confidential information or even seemingly non confidential information about you, whether it's over the phone, online, unless you can first verify the identity of the person asking and the need for that person to have that information. Also use strong and different passwords for your accounts, monitor your accounts and personal data, regularly backup your compute or create restore points, use unique security questions that can't guess.



Email / IM / Bulletin Boards

Hackers use malicious programs to steal sensitive information such as passwords and bank information. These email include malware attachment a program that can harm your personal computer. Always use a different password for primary email address than you would for a casual account or a random online registration. Keep passwords and username in a secured location known only to you. Have a minimum of 2 email addresses; one for professional matters and others for junk and spam mail or social media. Enable your anti-virus program to monitor your email account(s) and attachments. Finally, do not open mail from anonymous senders. Also download attachments from an email unless you were expecting to receive from trusted sender. Always remember to log out when using a computer other than your personal device. Learn tactics to identify suspicious email via cyberdrip.com.

Subscribe https://www.cyberdrip.com/ for gamified, simplified and online training programs

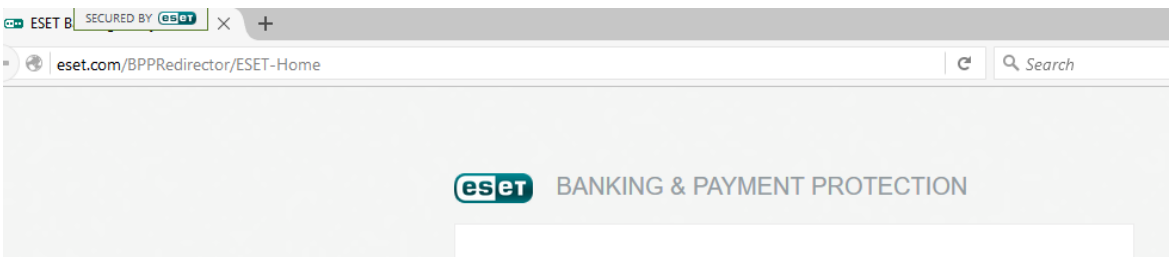


Web Browser

Your web browsing is the most important tool to be secured, Install an effective ad/popup blocker. Always browse with an updated and effective anti-virus software. Do not save login information for browsing convenience on a browser that is not your personal machine. Never enter any personal or bank information in an unsecured network or untrusted website. To find the website is secured for transaction, always check SSL (https). Most trusted websites provide SSL verified symbol or if SSL enabled, display left side to the address bar on web browser check if SSL is green as shown in figure below. Highly recommended to use safer browser which provide by anti-virus programs for online transactions. Example: ESET, Kaspersky.

Example:HTTPS

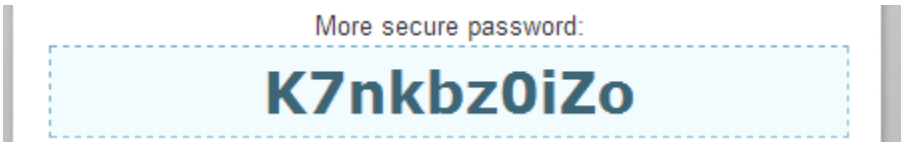
Example: Safe browser



Subscribe https://www.cyberdrip.com/ for gamified, simplified and online training programs

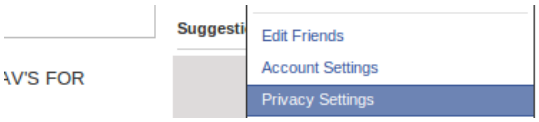
Complex passwords

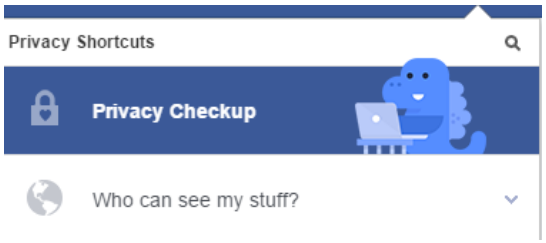
Most cyber criminals guess the password by your publicly available information. Avoid using birthday, pet name, your name, or default settings as your password. Always use complex password to avoid getting hacked. Always recommended to use both uppercase and lowercase letters include symbols and numbers. Password strength is most important part to avoid hackers to guess your password. Use minimum use 8 digits. Learn how to create secure and memoizable password via https://www.cyberdrip.com/.



Social Networking

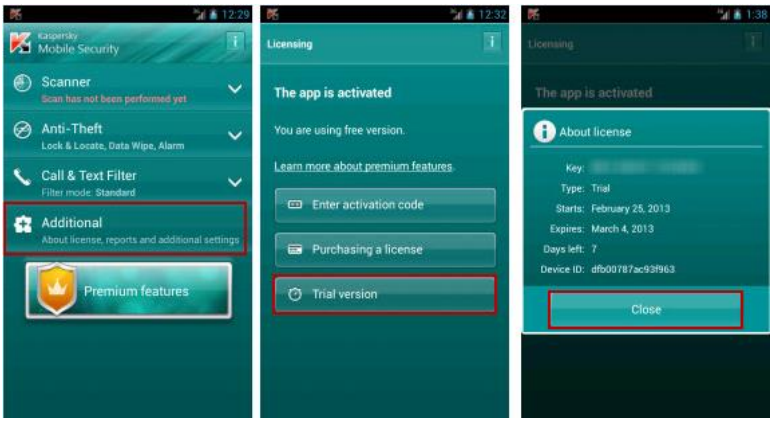
Since on social media, once something is posted, it is no longer private this can be impact on schooling and employment as well. Control who can see your information by adjust privacy settings so only "friends" can review your information. Always use a strong password and do not accept unknown friend requests. Please check your location on settings before publicly sharing personal life media.





Mobile device risks

Data leakage and theft or loss are some of the most common mobile risks. Lock your mobile device using password, fingerprint or pin. Update your apps and operating system to ensure that all security flaws have been worked out. Don't store sensitive data on devices or use public or unsecure Wi-Fi without the proper computer security. Protect your devices using mobile virus protection. Example: Norton mobile, Kaspersky, ESET mobile which available for all operating systems.



Encryption

Encrypt your external storage, and internal storage to add extra security layer to your storage. Purchase external flash drive which has the capability to encrypt using pin, password, or fingerprint. Learn more please visit https://www.cyberdrip.com/

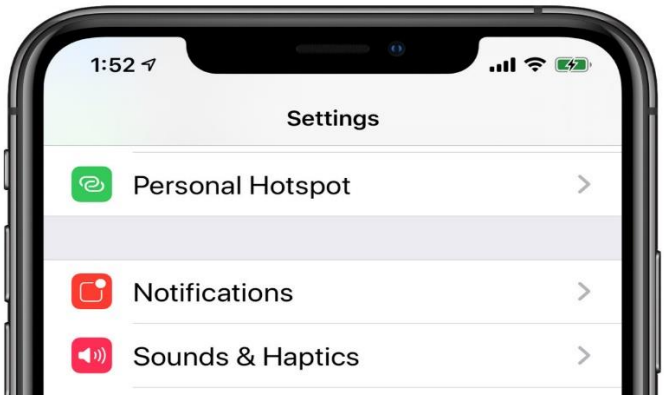
Data Destruction

If you need to remove all traces of a virus or you're planning on recycling or disposing of your hard drive or computer, wiping your hard drive using data destruction software is the best way to protect yourself. DBAN is free available software in a ready-to-go ISO format so all you need to do is burn it to a CD or flash drive and then boot from it. Please drill the drive before trash to avoid the risk of losing sensitive information.

Subscribe https://www.cyberdrip.com/ for gamified, simplified and online training programs

Remote working

Always use secured wife or wired connection between computer and the internet. Check if the WIFI connection public (multiple devices connected). Highly recommend to use mobile hotspot to create isolated network environment.

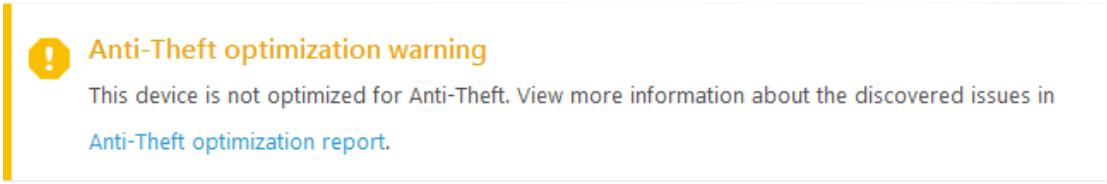


WiFi security and passwords

Use VPN enable secured wireless connection. When you connect to public WiFi network, VPN enable privet tunnel that encrypts data passes through the network. Vertual private network can help to prevent cybercrime. Most VPN providers charge $5 to $12 per month for high speed service as well. Purchase a provided allow to reset VPN. Example: NordVPN(Allow VPN reset via mobile), HideIPVPN, and OpenVPN.

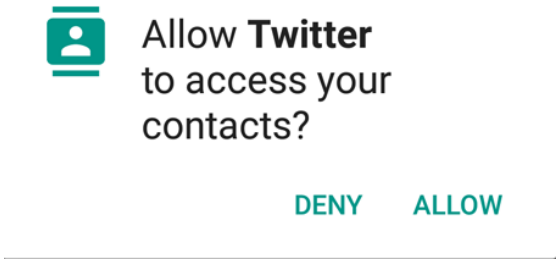
Physical device security

A laptop anti-theft product should keep your data safe, and keep away strangers from using the computer. It should protect your private data and resist a thief's attempts to disable its protection. Most Anti-virus software solutions provide Anti-theft program to track the location or trigger an alarm. It's highly recommended to enable the option in your anti-virus program. Example: Norton Symantec, ESET.



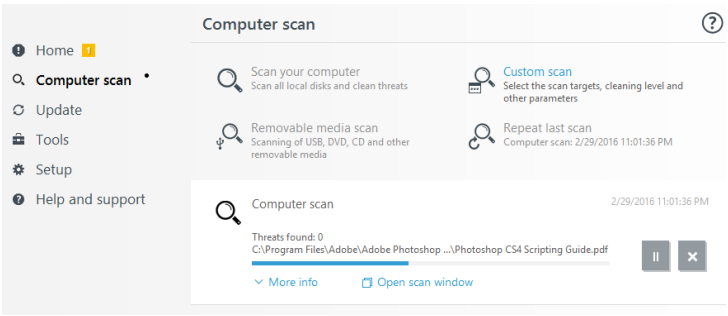
Apps permission

Disable unnecessary permissions by navigating to the apps settings. Such as share location, access to media, mic, camera, contacts etc. Simply disable to improve device security. (Applies for windows PC, IOS, and Android devices).



Got Hacked!

Even if you have one of the best anti-virus or internet security programs money can buy, hackers are clever and can find ways around programs such as untrusted cracked files which highly not recommend to use. Regularly run an in-depth scan of your entire computer system and update anti-virus protection. Change your passwords, and update your computer regularly.



Please visit cyberdrip.com to explore for version 2.0 web based gamified and skilled based training programs available on your fingerprints. Tool that can help you whenever you need cybersecurity guide.

By using our service for cyber-crime directly or indirectly prohibited by cyber security law. Strictly prohibited UNAUTHORIZED USE OF COMPUTER OR COMPUTER NETWORK. Please use measures and skills to defensive purposes only. This publication is unbiased review for some software products in the market.