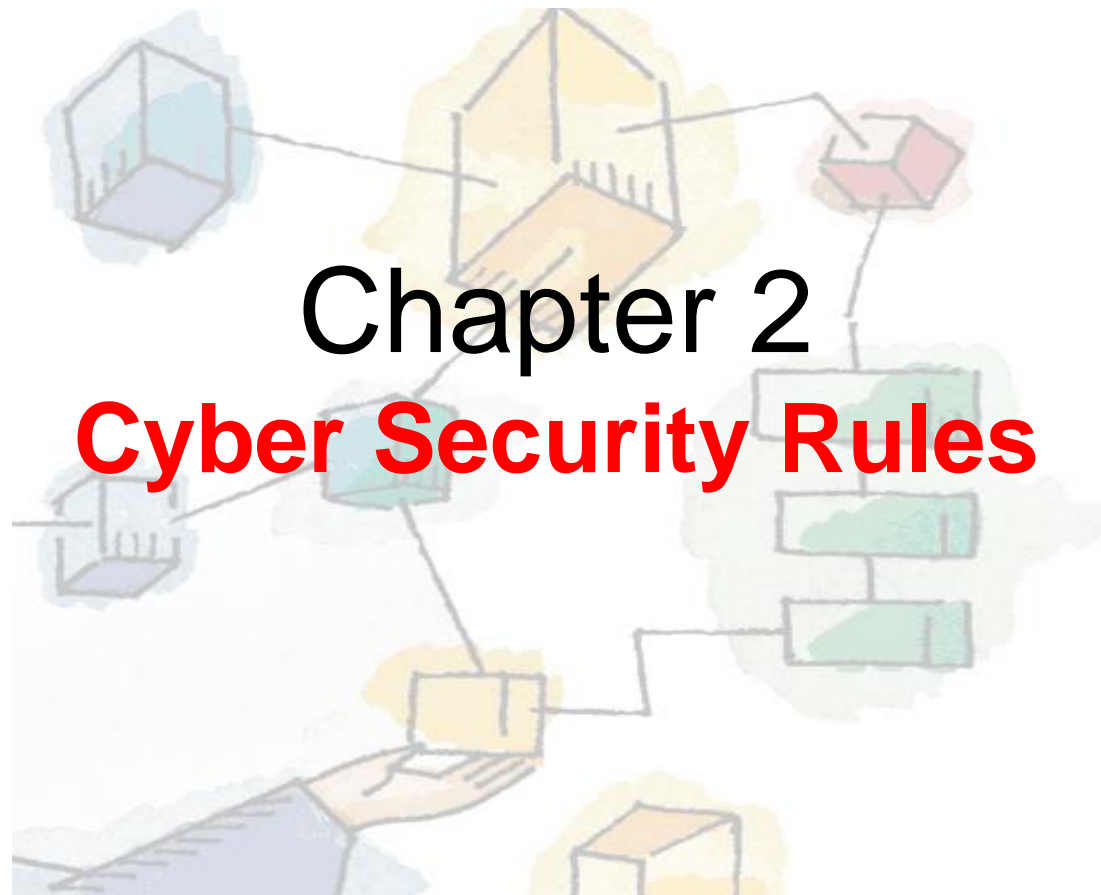


Cyber Security



Chapter 2

Cyber Security Rules

Cyber Security Rules

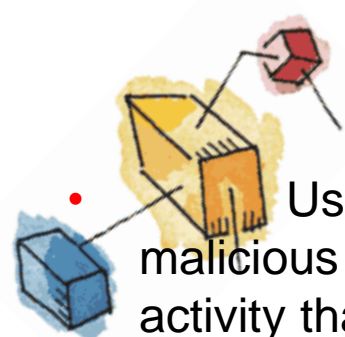
1. Keep Your Software Up to Date

- As we saw from the stats above, ransomware attacks were a major attack vector of 2017 for both businesses and consumers. One of the most important cyber security tips to mitigate ransomware is patching outdated software, both operating system, and applications. This helps remove critical vulnerabilities that hackers use to access your devices. Here are a few quick tips to get you started:
- Turn on automatic system updates for your device
- Make sure your desktop web browser uses automatic security updates
- Keep your web browser plug-in like Flash, Java, etc. Updated.

2. Use Anti-Virus Protection & Firewall

- Anti-virus (AV) protection software has been the most prevalent solution to fight malicious attacks. AV software blocks malware and other malicious viruses from entering your device and compromising your data. Use anti-virus software from trusted vendors and only run one AV tool on your device.
- This one speaks for itself but please always stay up to date with your software. Many updates these days do not only contain new features but are also security updates.

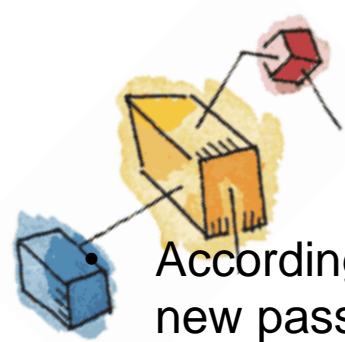
Cyber Security Rules



- Using a firewall is also important when defending your data against malicious attacks. A firewall helps screen out hackers, viruses, and other malicious activity that occurs over the Internet and determines what traffic is allowed to enter your device. Windows and Mac OS X comes with their respective firewalls, aptly named Windows Firewall and Mac Firewall. Your router should also have a firewall built in to prevent attacks on your network.
- Not updating means that known issues with your software are not taken care of and you are vulnerable to things that are commonly known as issues in the hacker community. This means also updating your wifi router firmware and other devices that are used in your network at the office or home. Please start using authorized antivirus programs with the support that really secures your devices (yes all of them). Not only your PC but also your phones and servers are at threat of attacks because hackers still can steal the information from your phones as they can to your PC.
- **3. Use Strong Passwords & Use a Password Management Tool**
- You've probably heard that strong passwords are critical to online security. The truth is passwords are important in keeping hackers out of your data!



Cyber Security Rules



According to the National Institute of Standards and Technology's (NIST) 2017 new password policy framework, you should consider:

- Dropping the crazy, complex mixture of upper case letters, symbols, and numbers. Instead, opt for something more user-friendly but with at least eight characters and **a maximum length of 64 characters**.
 - Don't use the same password twice.
 - The password should contain at least one lowercase letter, one uppercase letter, one number, and four symbols **but not the following &%#@_**.
 - Choose something that is easy to remember and never leave a password hint out in the open or make it publicly available for hackers to see
 - **Reset your password** when you forget it. But, change it once per year as a general refresh.
- Having a password is great and we assume that a password alone is enough to secure your data and privacy. Although this is true in some cases, many people tend to use the same password (or small variations of one) for all their systems and files. On top of that, we see that many passwords are quite weak and will take just a little effort for an average hacker to break them.



Cyber Security Rules

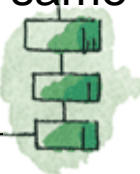
4. Use Two-Factor or Multi-Factor Authentication

Two-factor or multi-factor authentication is a service that adds additional layers of security to the standard password method of online identification. Without two-factor authentication, you would normally enter a username and password. But, with two-factor, you would be prompted to enter one additional authentication method such as a Personal Identification Code, another password or even fingerprint. With multi-factor authentication, you would be prompted to enter more than two additional authentication methods after entering your username and password.

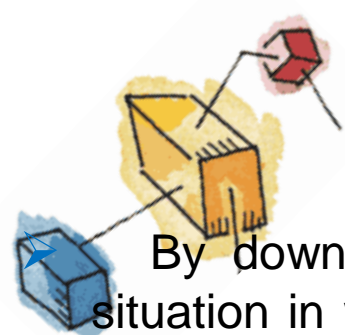
➤ **According to NIST**, an SMS delivery should not be used during two-factor authentication because malware can be used to attack mobile phone networks and can compromise data during the process.

➤ 5. Do not download illegal movies, music, or programs

➤ Many people have the habit of using free antivirus programs but it is commonly known that in a lot of those free products, there are traces of malware. Hackers, governments, and other parties use “free” products to gain access to your device. It is quite simple because users often allow these programs or files to be on the same disk where they store all the important files without any firewall or security.



Cyber Security Rules

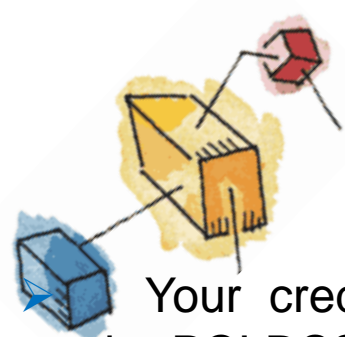


By downloading, installing, or using these products, you as a user, create a situation in which your antivirus will not work properly. Via this way key loggers are easily distributed to a large number of devices. The basic rule here is that “free” should be avoided and chosen for an official retailer.

- **6. Do not share your work devices with other people**
- Sharing your device with family, friends, or even others is not wise. Not only because they could want to harm you or your company, but simply because they do have not the same awareness of the risk they will encounter when they are using the device. It is a matter of responsible behavior. For example, a kid who just wants to play games easily goes from a game site via advertisements to bit more obscure sites. Installing a plug in to play a video or a game is easily done but the consequence could be quite severe. All the points of rule no. 5 could easily happen even if there is no bad intention.
- **7. Protect Your Sensitive Personal Identifiable Information (PII)**
- Personal Identifiable Information (PII) is any information that can be used by a cybercriminal to identify or locate an individual. PII includes information such as name, address, phone numbers, data of birth, Social Security Number, IP address, location details, or any other physical or digital identity data.



Cyber Security Rules



Your credit card information should be protected by companies if they follow the PCI DSS standards.

- In the new “always-on” world of social media, you should be very cautious about the information you include online. It is recommended that you only show the very minimum about yourself on social media. Consider reviewing your privacy settings across all your social media accounts, particularly Facebook. Adding your home address, birthdate, or any other PII information will dramatically increase your risk of a security breach. Hackers use this information to their advantage!
- **8. No one should have access to all data**
- As an owner and director, the first thing you always want is to have control over everything. This is one of the reasons you may be a good manager, but security-wise this is an issue. If you have staff and different departments make sure that the director cannot be the single point of failure. If a hacker targets a CEO, director, or owner successfully the whole organization could be in big trouble. Even in the military, for some heavy choices, there needs to be cooperation between multiple officers before an order can be carried out. Protect your organization and make sure no one could be the single point of failure of the entire organization.






Cyber Security Rules

9. Use Your Mobile Devices Securely

- According to McAfee Labs, your mobile device is now a target to more than 1.5 million new incidents of mobile malware. Here are some quick tips for mobile device security:
- Create a Difficult Mobile Pass code – Not Your Birthdate or Bank PIN
- Install Apps from Trusted Sources
- Keep Your Device Updated – Hackers Use Vulnerabilities in Unpatched Older Operating Systems.
- Avoid sending PII or sensitive information over text message or email.
- Leverage Find my iPhone or the Android Device Manager to prevent loss or theft.
- Perform regular mobile backups using iCloud or Enabling Backup & Sync from Android.
- **10. Close your social media account for strangers**
- This is a sensitive topic for a lot of people. For many, work says a lot of things about their private life or to some, their private life and work often are mixed up.



Cyber Security Rules

- 
- Only a handful of people can separate it to even a degree that the passwords will not be chosen in relation to someone close to them. To be safe for yourself, it would be good to not give total strangers all your personal information. Information via social media is a great source for phishing and creating a profile for identity theft. Once someone takes bad actions under your name, it is very hard to recover and to prove that action was not taken by you because they have all your identity information.
 - **11. Use common sense and make cyber security rules an open topic to discuss**
 - Your behavior is based on your common sense. Create an environment where people will want to talk about this subject. A place where people want to report incidents without being punished or laughed at. Since this is something everyone should be aware of and anyone can be a target, it is important that the management and IT department get every signal to build up a clear risk profile and can take countermeasures. Most attacks succeed because people are not noticing or alerting their managers. Once you see your device is under attack or strange things are happening there are two important steps:
 - **1: Disconnect from the network and internet**
 - **2: Warn the IT department and manager**



Cyber Security Rules




12. Backup Your Data Regularly

- Backing up your data regularly is an overlooked step in personal online security. The top IT and security managers follow a simple rule called the 3-2-1 backup rule. Essentially, you will keep **three** copies of your data on **two** different types of media (local and external hard drive) and **one** copy in an off-site location (cloud storage).
- If you become a victim of ransomware or malware, the only way to restore your data is to erase your systems and restore with a recently performed backup.

13. Don't Use Public Wi-Fi

- Don't use a public Wi-Fi without using a Virtual Private Network (VPN). By using VPN software, the traffic between your device and the VPN server is encrypted. This means it's much more difficult for a cybercriminal to obtain access to your data on your device. Use your cell network if you don't have a VPN when security is important.

14. Review Your Online Accounts & Credit Reports Regularly for Changes

- With the recent Equifax breach, it's more important than ever for consumers to safeguard their online accounts and monitor their credit reports. A credit freeze is the most effective way for you to protect your personal credit information from cyber criminals right now. Essentially, it allows you to lock your credit and use a personal identification number (PIN) that only you will know. You can then use this PIN when you need to apply for credit.
- 
- 