10 Cybersecurity Best Practices

The US and its numerous business' and computer systems are under heightened threat due to the current situation with the Coronavirus Pandemic and the need to work from home. Please carefully read this document completely.

Cybersecurity best practices encompass some general best practices — like being cautious when engaging in online activities, abiding by company rules, and reaching out for help when you encounter something suspicious. Here's a deeper dive into the 10 cybersecurity best practices for businesses that every employee should know and follow.

1. Protect Your Data

In your daily life, you probably avoid sharing personally identifiable information like your Social Security number or credit card number when answering an unsolicited email, phone call, text message, or instant message. It's important to exercise the same caution at work. Keep in mind that cybercriminals can create email addresses and websites that look legitimate. Scammers can fake caller ID information. Hackers can even take over company social media accounts and send seemingly legitimate messages.

It might sound obvious, but it's important not to leak your company's data, sensitive information, or intellectual property. For instance, if you share a picture online that shows a whiteboard or computer screen in the background, you could accidentally reveal information someone outside the company shouldn't see.

By the same token, be careful to respect the intellectual property of other companies. Even if it's accidental, sharing or using the IP or trade secrets of other companies could get both you and your company into trouble.

Your company can help protect its employees, customers, and data by creating and distributing business policies that cover topics such as how to destroy data that's no longer needed and how to report suspicious emails or ransomware.

2. Avoid: pop-ups, unknown emails, links in email and removable media

Beware of phishing. Phishers try to trick you into clicking on a link that may result in a security breach.

Phishers prey on employees in hopes they will open pop-up windows or other malicious links that could have viruses and malware embedded in them. That's why it's important to be cautious of links and attachments in emails from senders you don't recognize. With just one click, you could enable hackers to infiltrate your organization's computer network.

Here's a rule to follow: Never enter personal or company information in response to an email, pop-up webpage, or any other form of communication you didn't initiate. Phishing can lead to identity theft. It's also the way most ransomware attacks occur. Your company can help by employing email authentication technology that blocks these suspicious emails. You'll usually be notified that the email has been sent to a quarantine folder, where you can check to see if it's legitimate or not.

Be cautious. If you're unsure about the legitimacy of an email or other communication, always contact your security department or security lead.

NEVER plug in and USE removeable media of an unknown origin. If you find a USB Thumb drive anywhere never plug it in to your PC to see what is on it. Never plug in any removable media device to your PC if you do not know where it came from. This includes CD/DVD, Memory Cards, Micro Flash Drives, Flash Drives or any other removable storage devices. Attackers can place hidden files on a storage device that will activate upon insertion on a PC, the hidden files on one of these devices can spread virus', crypto-locker or even a "phone home" application that can contact the hacker directly from your pc and provide the hacker with direct access to your home or worse office computing network. This type of scenario has been used by attackers/hackers successfully immeasurable times to penetrate many companies, even fortune 500 companies. No one is immune to this type of social engineering attack.

3. At a minimum, Use strong password protection and authentication or significantly better, use Pass Phrases and Two-Factor authentication

Strong, complex passwords can help stop cyberthieves from accessing company information. Simple passwords can make access easy. If a cybercriminal figures out your password, it could give them access to the company's network. Creating unique, complex passwords is essential.

A strong password contains at least 14 characters and includes numbers, symbols, and capital and lowercase letters. Companies also should ask you to change your passwords on a regular basis. Changing and remembering all of your passwords may be challenging. A password manager can help.

Companies may also require multi-factor authentication when you try to access sensitive network areas. This adds an additional layer of protection by asking you to take at least one extra step — such as providing a temporary code that is sent to your smartphone — to log in.

3 passphrase best practices

- Be unpredictable: A strong passphrase is a random combination of words that are meaningless together. ...
- Do not reuse: No matter how strong your password may be, its appearance in a password dictionary makes it an easy target for hackers. ...
- Enable MFA: When in doubt, add another layer of authentication.

PASSPHRASE COMPLEXITY GUIDELINES

Requirement

When passphrases are used, they must meet the following complexity specifications:

Passphrases MUST:

- Contain eight characters or more
- Contain characters from two of the following three-character classes:

1. Alphabetic (e.g., a-z, A-Z)
2. Numeric (i.e. 0-9)
3. Punctuation and other characters (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

Multi-user systems must be configured to enforce these complexity requirements and require that users change any pre-assigned passphrases immediately upon initial access to the account.

All default passphrases for access to network-accessible accounts must be changed at time of network connection.

Background and description of risk

For many systems, passwords are the sole form of authentication. Poor password complexity, including insufficient length or the inclusion of commonly used words, may allow an attacker to guess the password and gain unauthorized access to the system. Generally, the more complex the password, the more difficult it is for an attacker to guess. A password guess is not a person guessing your password. A guess is normally performed by a computer using an automated application that uses an algorithm to process millions of password guesses in minutes.

In addition, failing to change passwords from the default vendor/manufacturer settings is equivalent to having no password at all, as default passwords are commonly known by attackers. Most devices that are purchased for computing use have default manufacturer usernames and passwords that are published on the manufactures support website and are accessible by anyone with an internet connection.

RECOMMENDATIONS

Passphrases **SHOULD NOT** be:

- A derivative of the username
- A word found in a dictionary (English or foreign)
- A dictionary-word spelled backwards
- A dictionary-word (forward or backwards) preceded and/or followed by any other single character (e.g., secret1, 1secret, secret? and secret!)

When might it be inappropriate to configure my device to enforce the minimum password complexity requirements?

It may be inappropriate in situations where the device is single user (home machines or laptops). While you MUST use a password that meets the complexity requirements, it is not necessary to configure the device to enforce the requirements on these single-user devices.
Aside from the password requirements in the Minimum Standards document, what are some other guidelines I should follow?

- Do not use an easily guessed password. Some examples of passwords that would be easy to guess:
    - Names of family, pets, friends, co-workers, and hobbies etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

- Passwords should never be written down or stored on-line.
- In general, a password should be as long as possible while still being easy-to-remember.
- Use simple to remember phrases, for example (Isee3pinkducks!) or (IlovemyL@ndrover2)
- One way to do this is create a password based on an easy-to-remember phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use any of these examples as passwords!
- You should always change your passwords on a regular basis, at least every six months. You should also change your password any time you suspect that your account has been compromised or tampered with, do not assume you are just being paranoid. If something with your computer seems wrong or out of place CHANGE YOUR PASSWORD IMMEADIATLY!
- Try to use a different password for every system, and every application you use. At a minimum, do NOT use the same password for any of your accounts that you use for a non- work/service or third-party web site.

4. Connect to secure Wi-Fi

Office Wi-Fi networks should be secure, encrypted, and hidden. If you're working remotely, you can help protect data by using a virtual private network, if your company has one. A VPN is essential when doing work outside of the office or on a business trip. Public Wi-Fi networks can be risky and make your data vulnerable to being intercepted. Never connect to a work/office computing system from a public Wi-Fi system without a VPN connection, never.

But keep in mind, some VPNs are safer than others. If your company has a VPN it trusts, make sure you know how to connect to it and use it. VPN provides powerful secure encrypted tunnel protection that can help keep your information private on public Wi-Fi.

5. Enable firewall protection at work and at home

Employees working from home, the risk is increased as you blend your home network with your work network. This portion of the document will help to clarify the elevated risks that come with working from home.

Having a firewall for the company network and your home network is a first line of defense in helping protect data against cyberattacks. Firewalls prevent unauthorized users from accessing your websites, mail services, and other sources of information that can be accessed from the web. Most Internet Service Provider modems have built in firewalls. They are not as secure as a separate Firewall appliance, but they are much better than an open internet connection from home. Secure your firewall at home. Your Home PC has much more information that can be used to profile you or the company you work for.

Accessing your home modem is not difficult by a hacker if the firewall is not configured and turned on. Most modems used by ISP's have user guides to assist you in configuring your home ISP Modem's firewall. If you require assistance call us and we can assist you. Please consider Pioneer your home IT support professionals.

They can go around the VPN connection and access your home computer then use the VPN you are connected too to access your employers' network. So, if attackers can't get into your ISP modem then they can't get to your home PC or any other device on your home network. Install a firewall on your home network if you work from home. Ask your company if they provide firewall software. Many software vendors provide firewalls that are preconfigured and easily managed to protect your PC, Symantec/Norton Internet Security is very user friendly and inexpensive.

6. Invest in security systems

Smaller businesses might hesitate when considering the cost of investing in a quality security system. That usually includes protections such as strong antivirus and malware detection, external hard drives that back up data, and running regular system checks. But making that investment early could save companies and employees from the possible financial and legal costs of being breached. All of the devices you use at work and at home should have the protection of strong security software. It's important for your company to provide data security in the workplace but alert your IT department or Information Security manager if you see anything suspicious that might indicate a security issue. There may be a flaw in the system that the company needs to patch or fix. The quicker you report an issue, the better.

7. Install security software updates and back up your files, Patching is your Number 1 defense against hackers.

Following IT security best practices means keeping your security software, web browsers, and operating systems updated with the latest protections. Antivirus and anti-malware protections are frequently revised to target and respond to new cyberthreats.
If your company sends out instructions for security updates, install them right away. This also applies to personal devices you use at work. Installing updates promptly helps defend against the latest cyberthreats.

Cyberthreats often take aim at your data. That's why it's a best practice to secure and back up files in case of a data breach or a malware attack. Your company will probably have rules about how and where to back up data. Important files might be stored offline, on an external hard, drive, or in the cloud.

8. Talk to your IT department/support

Your IT department is your friend. Reach out to your company's support team about information security. You might have plenty to talk about.

It's a good idea to work with IT if something like a software update hits a snag. Don't let a simple problem become more complex by attempting to "fix" it. If you're unsure, IT can help.
It's also smart to report security warnings from your internet security software to IT. They might not be aware of all threats that occur.

It's also important to stay in touch when traveling. Let your IT department know before you go, especially if you're going to be using public Wi-Fi. Have a great trip — but don't forget your VPN.
Remember to make sure IT is, well, IT. Beware of tech support scams. You might receive a phishing email from someone claiming to be from IT. The goal is to trick you into installing malware on your computer or mobile device or providing sensitive data. What to do? Don't provide any information. Instead, contact your IT department by phone right away.

9. Employ third-party controls

Here's a fact that might be surprising. It's common for data breaches to begin from within companies. That's why organizations need to consider and limit employee access to customer and client information.

You might be an employee in charge of accessing and using the confidential information of customers, clients, and other employees. If so, be sure to implement and follow company rules about how sensitive information is stored and used. If you're in charge of protecting hard or soft copies, you're the defender of this data from unauthorized third parties.

Companies and their employees may also have to monitor third parties, such as consultants or former employees, who have temporary access to the organization's computer network. It's important to restrict third-party access to certain areas and remember to deactivate access when they finish the job.

10. Embrace education and training

Smart companies take the time to train their employees. Your responsibility includes knowing your company's cybersecurity policies and what's expected of you. That includes following them. If you're unsure about a policy, ask.

Here's an example. Maybe you wear a smart watch at work. It's important to protect personal devices with the most up-to-date security. You'll also want to know and follow your company's Acceptable Electronic Use (AEU) policy. When you Bring Your Own Device — also known as BYOD — ask your IT department if your device is allowed to access corporate data before you upload anything to it. Always be sure to use authorized applications to access sensitive documents. Never use a USN Thumb drive/jump drive to download company information for use on your personal device.
A little technical savvy helps, too. Learning the process for allowing IT to connect to your devices, along with basic computer hardware terms, is helpful. That knowledge can save time when you contact support and they need quick access and information to resolve an issue.
If you want to back up data to the cloud, be sure to talk to your IT department first for a list of acceptable cloud services. Organizations can make this part of their AEU policy. Violation of the policy might be a cause for dismissal.

YOU CAN PREVENT A DATA BREACH, BY USING COMMON SENSE A HEIGHTENED SENSE OF AWARENESS AND SUSPICION OF ABNORMAL EVENTS WHILE COMPUTING! IF IT LOOKS ODD OR OUT OF PLACE IT LIKELY IS WORTH REPORTING IMMEDIATELY!

Having the right knowledge — like the 10 cybersecurity best practices that every employee should know — can help strengthen your company's breach vulnerabilities. Remember: just one click on a corrupt link could let in a hacker. Just one failure to fix a flaw quickly could leave your employer vulnerable to a cyberattack.

It's part of your job to engage in safe online behavior and to reach out to your IT department when you encounter anything suspicious or need help.

Staying on top of these cybersecurity practices could be the difference between a secure company and one that a hacker might target.