Industry Best Practices to Protect Employees and Company Assets

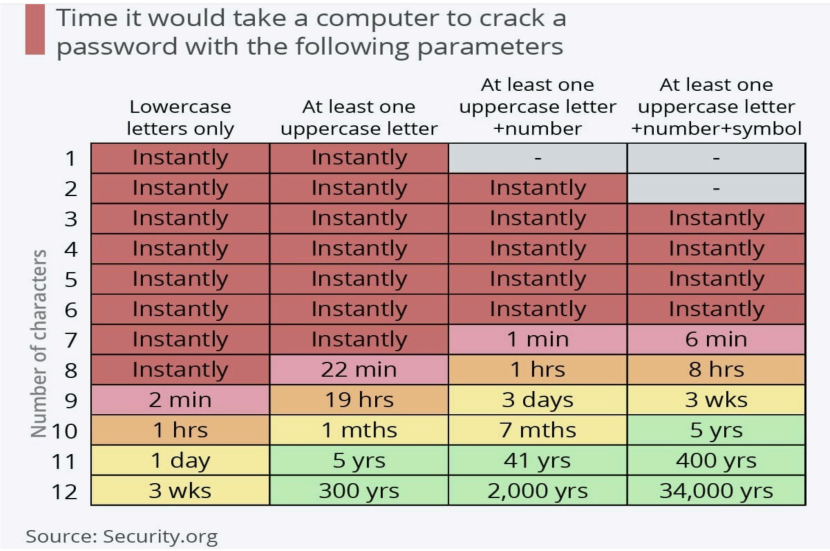
Executive Summary

To help secure the valuable information of the company and its employees, we must ensure that everyone is following the basic principles of security also known as the industry best practices. In this report we will go over each of these elements and go over why implementing these best basic security measures will enable the company to take the step forward in the right direction to protecting the employees as well as the companies valuable assets. The industry best practices are as follows:

- Strong password.
- Password expiration policy.
- Multi-Factor Authentication (MFA)
- Secure email with a personal certificate.
- VPN IPsec on the laptops for remote connections.
- Encrypting hard and flash disks to protect portable/mobile devices.

Strong Passwords

When it comes to securing the employees accounts which connect to the companies network, having a strong password is the first line of defense. Depending on the complexity and length of the password, a malicious attacker can take anywhere from instantly breaking through a password to 34 thousand years according to '*World Economic Forum'*. The industry best practice is to have employees set up their password with 10 - 12 characters while containing at least one upper case, number, and symbol, for it to take as long as possible for a malicious attacker to attempt to acquire the password.



	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

The chart depicts how long it would take a computer to acquire a password based on complexity.

Password Expiration Policy

When employees set up their passwords they are secure from any malicious attacker from gaining access to their account by just logging in as the employee. But what happens when a malicious attacker attempts to use a computer program or AI to acquire the password via a brute force attack? In this case, a policy that will further secure passwords and accounts for employees is the '*Password Expiration Policy'*. When an employee creates a password that has at least 10 characters containing at least one uppercase letter and 1 number, according to the chart above it takes roughly 7 months for the computer to acquire a password. Using this information enacting a policy that requires employees to change their password periodically will make the malicious attackers efforts to obtain a password. The recommended time for an employee to change their password based on this policy, is at least 60 days or 90 days. The password length and complexity combined with this policy will make it harder for malicious attackers to acquire the password by using a brute force method.

Multi-Factor Authentication (MFA)

Now that the possibility of brute force attacks has been significantly lowered, the next type of common attack or vulnerability that we can defend against is a phishing attack. Phishing attacks occur when a malicious attacker attempts to acquire information by sending an email claiming to be someone else. For example, an attacker can pose as a member of the security team asking for login information. To Prevent this type of attack while securing the employee's account we will use Multi-Factor Authentication (MFA), to provide an extra layer of employee authentication when logging in. MFA is implemented after an employee attempts to login with their password, password recovery, and password reset. MFA comes in many different forms whether it be, sending a text message or email with a verification code, captcha prompts to verify that a computer did not access the account, sending an email with a warning of an account login, etc. Implementing MFA ensures that when a malicious attacker attempts to login on an employees account, that the employee will be notified of the compromise and will take action to change their password, and notify the security team or management.

Secure Email With a Personal Certificate

After securing user accounts, ensuring we can securely send important files between users is vital. There are various attacks that target data being transferred between users on a network. One such attack is named the “Man-in-the-Middle” attack in which an attacker can intrude and corrupt communications between users. Keeping this in mind, the way we can combat these types of attacks is by using a personal certificate to encrypt email correspondence. A personal certificate is a way for employees and managers to include people in an email. When the personal certificate is set up, only those who are included in the email will be able to access it with a password key and sign the documents. Not only does a personal certificate ensure that employees who are included in the email can see it, the certificate will also encrypt the files when sent so only those employees with the password key can access it. Setting up this level of security is relatively easy, and it would incorporate help from the network administrative team for some further assistance on setting up the personal certificate. The general process is as follows:

1. **Acquire a Digital ID**: This requires the aid of a digital signature service like digicert.

2. **Specify the Digital ID to use**: This is where the company can set up the encryption method to use.

3. **Adding Recipients DIgital ID to Contacts**: Other employees will gain their digital ID which will allow them to be added to the correspondences.

Using a personal certificate for emails will allow important correspondences to remain secure between employees, and prevent attacks such as the “Man-in-the-Middle” attacks.

VPN IPsec on Laptops for Remote Connections

Encrypting data for employees using the network and emailing within the home network, but we also need to ensure that we can secure file transfers and other important data transfers for remote employees. VPN (Virtual Private Network) is used to mask the IP of the computer and where it will send data remotely. Often used on company devices like laptops, to have secure communication between the source of the correspondence, and where they send information too. A VPN is great for masking where the origin and destination of where data is being sent, but the data itself is still vulnerable to attacks like the “Man-in-the-Middle” attack described above. To combat this, VPN’s are normally used in conjunction with an encryption tool called an IPsec (Internet Protocol Security). IPsec is an extra tool that takes files being sent and received, and encrypts the data to allow the files to not be easily corrupted by malicious attackers when being sent. Similar to how the personal certificate works, IPsec provides secure communication with remote employees accessing the network as well as distributing the files remotely.

Encrypting Hard and Flash Disks to Protect Portable/Mobile Devices

Encrypting the areas where data can be stored such as the hard drive or flash disks will help secure the data stored within the devices even if the computer, mobile device, laptop, etc is accessed by a malicious attacker. Encrypting these devices can be relatively simple as well, sometimes devices will come with an option to enable an encryption for the built in hard drive of the computer. Other times where this option is not available, using external software such as BitLocker will allow the user to encrypt the built in hard drives, as well as any external hard drives. This allows for a secure place where any important data is able to be stored and accessed only by those with the password key to the hard drive or flash disks.

With these basic security measures and policies in place, it will be harder for malicious attackers to gain access to employee information and company data, using any of the common attack types. Following these simple protocols will enable the security team, and any other network administrative teams, to patch other important vulnerabilities found in a timely manner.

Work Cited

Buchholz, K. (n.d.). *This chart shows how long it would take a computer to hack your exact password*. World Economic Forum. https://www.weforum.org/agenda/2021/12/passwords-safety-cybercrime/

Microsoft. Microsoft Support. (n.d.). https://support.microsoft.com/en-us/office/get-a-digital-id-0eaa0ab9-b8a2-4a7e-828b-9bded6370b7b

Stouffer, C. (n.d.). *What is a man-in-the-middle attack?*. India (English). https://in.norton.com/blog/wifi/what-is-a-man-in-the-middle-attack

Microsoft 365. (2022, December 29). *How to encrypt a USB flash drive-and why you should*. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-and-why-to-encrypt-usb-flash-drive