Security Awareness Training 2019

# Tips and Suggestions to Improve Security Awareness

## Quick Summary

Score: 74%

Security Rating: C

## Security Tips

|  |  |
| --- | --- |
| Topic | Tip |
| Password Creation | When creating a new password, you should follow these best practice rules:  Include - 12+ characters, upper and lower case letters, numbers, special characters.  Not Include - Personal information such as birthdays and names of pets and family, words that can be found in a dictionary, and any repeated sequences of letters or numbers. The reason for this is because it is easy for hackers to find personal information about you such as your birthday, names of your family members, and the names of your pets. Additionally, try not to include words that are found in a dictionary because hackers can use a simple algorithm to plug in words in an attempt to break your password. Overall, the best passwords are unique passwords. |
| Physical Access | Whenever you leave your desk you should always lock your computer and take your badge with you. Even if you are leaving for “just a second”, it only takes a hacker or rogue employee one second to take a badge. Additionally, you should never hold doors open unless the employee has a security badge. Too often, people with malicious intent are able to pose as if they work for the company and gain access by following others through the doors. |
| Data Encryption | Sensitive data should always be encrypted without exception. This is especially true when sending information to others through less secure means such as email. |
| Phishing | First off, you should always check the email addresses of emails that you receive. Hackers will try and send you emails that appear that they are from legit sources when in fact, they slightly altered the email address. Additionally, if you find emails from outside sources in your inbox that you do not recognize, you should exercise the utmost caution. You should never open suspicious emails or open suspicious email links. More often than not it is a hacker trying to put malicious software on your computer and/or gain information. If you think you received a phishing email, notify your cybersecurity group. |
| VPN vs. Public Network | Public WiFi Networks are not the safest to connect to. Your data is vulnerable to hackers and could be intercepted. When working outside of the office, it is best to connect to a VPN (Virtual Private Network). VPN’s are safe, secure, encrypted, and hidden. |