Name of training: Passwords – Making strong ones and managing them

Purpose of training: To teach people how to build and manage secure passwords for account protection

Audience: All office staff

Why is this important to learn? 123456 is one of the most common passwords stolen and misused. People need to know how to create and manage their passwords in a way that protects them.

Content to cover:

Intro about passwords	Passwords are the main way you can protect your accounts and online identity. They're more important than ever, and most people don't have good ones. Most people have the same password for a majority, or all, of their accounts. If their password is stolen once, the criminals have access to all their accounts and will take over their LinkedIn, Facebook, email accounts, and anything else they can find. According to some cyber security researchers, there may be over 20 billion stolen passwords being sold and shared on the dark web. Cyber criminals are buying these passwords and using them to log in to people's accounts.
Common bad passwords for online accounts/apps/3rd parties	The 10 most common passwords that appear in the 20+ billion stolen password troves are: 123456, 123456789, Qwerty, 12345, Password, Qwerty123, 1q2w3e, 12345678, DEFAULT, and 111111. Passwords requirements for websites and apps are typically a minimum of 8 characters long, and have a letter, number and symbol – this isn't good enough any more.
Passwords minimums at [redacted]	For your Login and email account at [redacted], your password must be at least 15 characters long, which is a great start, but it could still be a bad password. e.g. passwordpassword!1 is a weak password.
Passwords that are a scramble	Historical password advice says to have a scramble of letters, numbers, and symbols. If your password is a long scramble such as the below, it is strong. It is very hard to remember, however. X3r$k15wBm9*Pa38 < strong but hard to remember
[activity]	Which is stronger: Company123! OR obgsw#24oi3nb
Passphrases are better than passwords	Passphrases are currently best practice. Using 3 or 4 words, a number, and a symbol, is easier to remember and very strong. Repeating any words weakens the password. LinkedinHappyRockingHorse18# < easier to remember, and strong. JumboWaterBoatTime256$ < also very strong.
[activity]	Which is stronger:

	obgsw#24oi3nb OR PeanutButterJellyTime261#
Using the same password for everything	According to a Google survey over half of people have the same password for most accounts, and many have the same password for everything. Why is this bad? Well, let's say you use the password "Company123!" for most of your online accounts. If it's stolen from one place, then a criminal could access your other accounts. Where are the passwords stolen from? Unfortunately, many companies have been breached over the years, and during these breaches, criminals have sometimes successfully stolen usernames and passwords. If a website or app you use has been breached, it's possible your username and password are available for purchase!
Anatomy of hackers stealing and selling details	[FlowDiagram1.png]
Haveibeenpwned.com	To check if your details are being sold online, security researchers find many of these lists, buy/download them, and then let you check your email account to see if your details are being sold online and where they were stolen from. You just need to go to https://haveibeenpwned.com – enter your email account/s and then change any passwords for websites or apps that have been breached – and if you use the same password elsewhere, change it there too otherwise criminals may try to log in to your other accounts.
What about saving your passwords on your computer?	It's also advised not to save all your passwords in a file on your computer. If malware infects your computer, it may steal that file and then the criminals would have access to your accounts.
Are password managers something I should look in to?	Password managers to make life easier. A password manager is a dedicated app that you install on your phone and install the extension for in your browser. You only need to remember one password to be able to access the password manager, and then it does the rest! All your passwords can be very long, a scramble, and unique, and you don't have to remember any of them. Some of the most reputable ones are LastPass, DashLane, and 1Password. There are others that are also good and we recommend checking out a couple to see which could work best for you, and even your family.
Video on using a password manager?	Can we just use youtube embedded? https://www.youtube.com/watch?v=xHSnHj-zKF4
What if my password still fails?	If your password is stolen through a malware (spyware) attack or a sophisticated phishing attack, Multi-factor Authentication is your backup defense to stop criminals from accessing your account/s. Multi-factor Authentication relies on two different ways to determine its actually you trying to log in. It will use something you know (your username and password) and then something you have (usually your phone by SMS or Authenticator App).
Ending Quiz	

1	When criminals hack into companies' websites and apps they may steal usernames and passwords: True OR False
2	Which one of these is a passphrase (and stronger than a traditional password)? ☐ Password1! ☐ TruckTruckTruckTruck123 ☐ PutTheLimeInTheCoconut38# ☐ D7J*e3#3oije
3	Which things are most important about passwords? ☐ Making them unmemorable ☐ Making them long ☐ Not using easy and common passwords ☐ Keeping them all unique
4	What's the easiest and most secure way to manage passwords ☐ Writing them down on paper ☐ Writing them down in a word/notes document ☐ Use a few different passwords ☐ Use a password manager to generate and store all your different passwords
5	MFA stand for: ☐ Multiple For Access ☐ Multi-factor Authentication ☐ Minute-factor Application
6	MFA: ☐ Stops all malware from being installed ☐ Stops someone logging into your account if they've stolen your username and password ☐ Means passwords don't matter anymore