Which of these is NOT a way to make a strong password?

Using your birthday and name (Correct)

Turning a sentence into a password

Add punctuation to a password

Make a long password

Using information that people maybe able to find out about you is not a good idea.

Which of the following is the stronger password?

P@5sW0rD (Correct)

password

1234password

23password!

While all the options can be uncovered by an attacker, P@5sW0rD is the stronger of the bunch as it requires more effort.

What would "Whispers of twilight linger, shadows dance beneath the Moon!" look like as a password?

Wotl,sdbtM! (Correct)

wotlsdbtm

WotlsdbM

wotl,sdbtm!

Using a sentence as a password means including all of the capitalisation and punctuation!

What should you try when setting up a password?

Utilizing the first letter of each word in sentence (Correct)

Using common song lyrics as password phrases

Including only lowercase letters and numbers in the password

Keep it short to make them easier to remember

Using a sentence to set up a password is a good way to make a password strong against dictionary attacks.

Which of the following would make a good sentence for a password?

"I can do anything? Even shuffle all the cards!" (Correct)

"May the force be with you."

"You’re a wizard, Harry!"

"Somebody once told me, the world is gonna roll me."

The choice of sentence for a password should be memorable like these, but it shouldn’t be something popular like a song or movie quote.

Which of the following is a characteristic of phishing attacks?

Targeting individuals to obtain sensitive information (Correct)

Targeting only computer systems

Typically involving physical intrusion

Exclusively conducted through social media platforms

Phishing attacks target people and are done through a wide array of places such as email, SMSs or social media.

Which is not a common way through which phishing attacks may occur?

Physical letters (Correct)

Email

SMSs

Web pages

Due the how quickly, and how automated, phishing attacks can be done, sending a message through email or SMS, or even creating a fake website, is most common.

What is NOT a way to spot a phishing link or account?

Looking for a business you know (Correct)

Misspelling in the account name.

Extra letters where there shouldn’t be

Switching letters for other letters or numbers

Spelling mistakes, extra letters and switched or swapped characters are common ways used to impersonate an account. If you look for a business name you know, the link may still be bad. For Example, while google.suport@email.com looks legitimate, such a google account would use gmail.com as the domain and has misspelled support.

How can phishing attempts often be identified?

They may exhibit signs of rushing the recipient (Correct)

They always come from a businesses

They are impossible to detect

They are exclusively caught by automated systems

Remember, automated systems may miss some phishing attempts and attackers can also impersonate people, not only businesses. They also try to rush you and have questionable account names imitating legitimate ones.

Which of the following is NOT an aim of phishing?

To provide you with free software (Correct)

To get you personal information

To gain access to one of your accounts

To get you to download malware

Phishing attempts aim to get your information, account and password or to download malware. Providing you with free software may be the claim made in a phishing attack, but it is not an aim.

You get an email from your friend, Digibot, through your school emails. Which of the following emails would you trust?

Digibot@school.edu (Correct)

Digibot@schoo1.edu

Digiboot@school.edu

Digibot@school.com

Always be vigilant for accounts adding extra letters, "Digiboot", using a different domain, "school.com". or swapping out letters, "schoo1". While these a could be blatant, swapping out an lower case L for an upper case i might be difficult to see.

What is the primary purpose of ransomware?

To demand payment for regaining access to the computer (Correct)

To render a computer unusable

To delete random files

To steal sensitive data

While ransomware does make a computer unusable, the main goal of it is to get payment from a victim.

What is a common function of spyware?

Stealing data and monitoring user activity (Correct)

Making a computer unusable

Deleting random files

Encrypting files and demanding ransom

Spyware is made to spy on you, see what you are doing and access information and send it to the attacker.

What caution should individuals exercise when downloading files from the internet?

Only download files from known and trusted sources (Correct)

Ignore the source of the file if it looks legitimate

Avoid files with extensions like ".exe" altogether

Always share downloaded files with others for verification

Files downloaded online should only come from a known and trusted source. You can’t ignore all exe files as some are legitimate and you should never send files you are suspicious of to others and rather delete them.

Why is it advised to be cautious when downloading files with the ".exe" extension?

Because the source of the file matters; files from unknown sources may be malware (Correct)

Because all files with ".exe" extension are malware

Because ".exe" files are harmless and should be freely downloaded

Because ".exe" files are exclusive to malicious websites

A file being an exe file is not enough to call it malware, where it comes from is an important factor to consider.