Lesson 1 Game: Be cautious when working in the office

Staff are unaware of the risks when working in the office. The purpose of this text-based adventure game is to educate users on how to maintain information security and web safe when working in the office.

Please enter your name:

---------------------

电脑游戏画面

中度可信度描述已自动生成

Welcome,

----------------------! This game is intended to help you understand the risks when working in the office. You can proceed the game by clicking the page. Each page will contain a scenario to guide you towards the next level. Once you start the game, you are required to fill in the blank, complete multiple-choice questions or true or false questions. After you are finished with the game, the number of correct answers will be shown in the end. They will be counted towards your final score. You can start your journey now!

电脑游戏画面

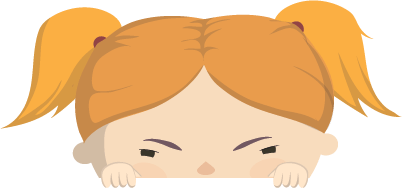
中度可信度描述已自动生成

Though you may feel like it’s an exciting and somewhat relaxing opportunity to work at office.

It is important to not carelessly let your security awareness down.



Take our lady Amy here for example.



She is working on some invoices in the office.

As you can see, there is a lot of sensitive information she is downloading.



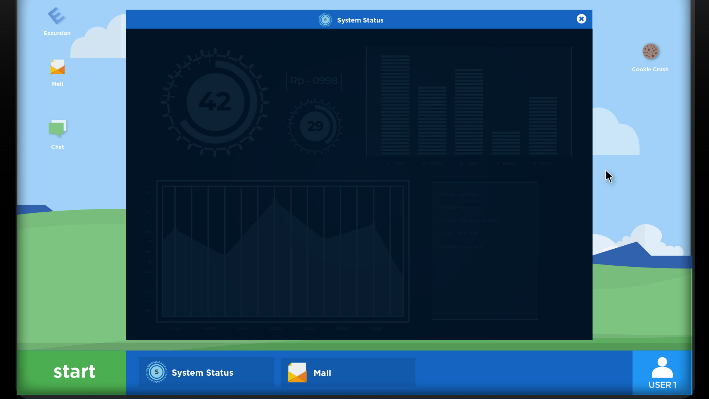
I hope it’s safely secure on her office computer.

Wait! All the invoices Amy has downloaded from office is sent directly to Tom.

卡通人物

描述已自动生成

But how?

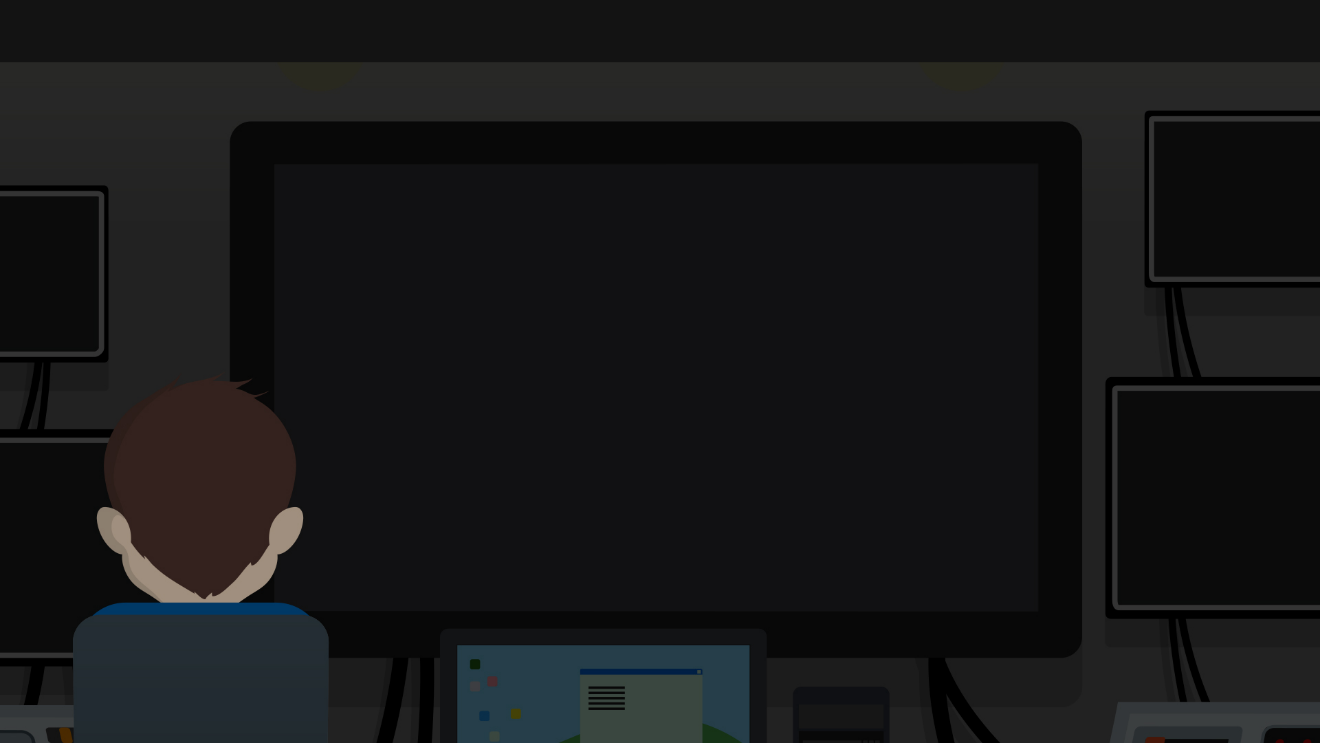


Let’s rewind all this mess.

What is the cause of downloaded files being sent directly to Tom?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer: The cause of downloaded files being sent directly to Tom is likely due to malware being installed on Amy’s computer.



Normally Amy has to maintain the security of her own devices when working in the office.

So, Amy, it looks like you need to take some more responsibility over security.

What should Amy do to prevent this from happening?

­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer: She should download and install an operating system update as soon as she is notified about it.

Make sure anti-virus software is up to date and running on the computer.

Executing these steps will often help patch any recently discovered security issues related to the devices.

矩形

低可信度描述已自动生成

Before we crack on with those invoices though, is your Wi-Fi network password protected and therefore safe from others freely connecting, by any chance?

I will check them.

I decline to check them.

Answer: I will check them.

Here, your knowledge of information security will be tested to check if you have fully understood the learning materials.

It is not your responsibility to be proactive about security when working in the office. Instead, the IT support team should ensure security of devices, data and the network.

True

False

Answer: False

Employees should download and install operating system updates as soon as they are available.

True

False

Answer: True

Staff should ensure that their antivirus is up-to-date and enabled.

True

False

Answer: True

Staff should protect their Wi-Fi network and router with strong passwords.

True

False

Answer: True



Congratulations! You have completed the game and successfully answered all the questions.

In lesson 1 game, you have answered \_\_\_\_\_\_\_ questions correctly. The number of correct answers will be counted towards your final score. Thank you for your participation and enjoy the learning of iSecurity Platform!

游戏机里面的人物

描述已自动生成

Lesson 2 Game: Using Public Wi-Fi Securely

Staff are often unaware of the risks when connecting to public Wi-Fi. The purpose of this text-based adventure game is to enlighten employees on the risks and educate them on how to stay safe.

Please enter your name:

---------------------



Welcome,

----------------------! This game is intended to help you understand the risks when connecting to public Wi-Fi. You can proceed the game by clicking the page. Each page will contain a scenario to guide you towards the next level. Once you start the game, you are required to fill in the blank, complete multiple-choice questions or true or false questions. After you are finished with the game, the number of correct answers will be shown in the end. They will be counted towards your final score. You can start your journey now!

电脑游戏画面

中度可信度描述已自动生成

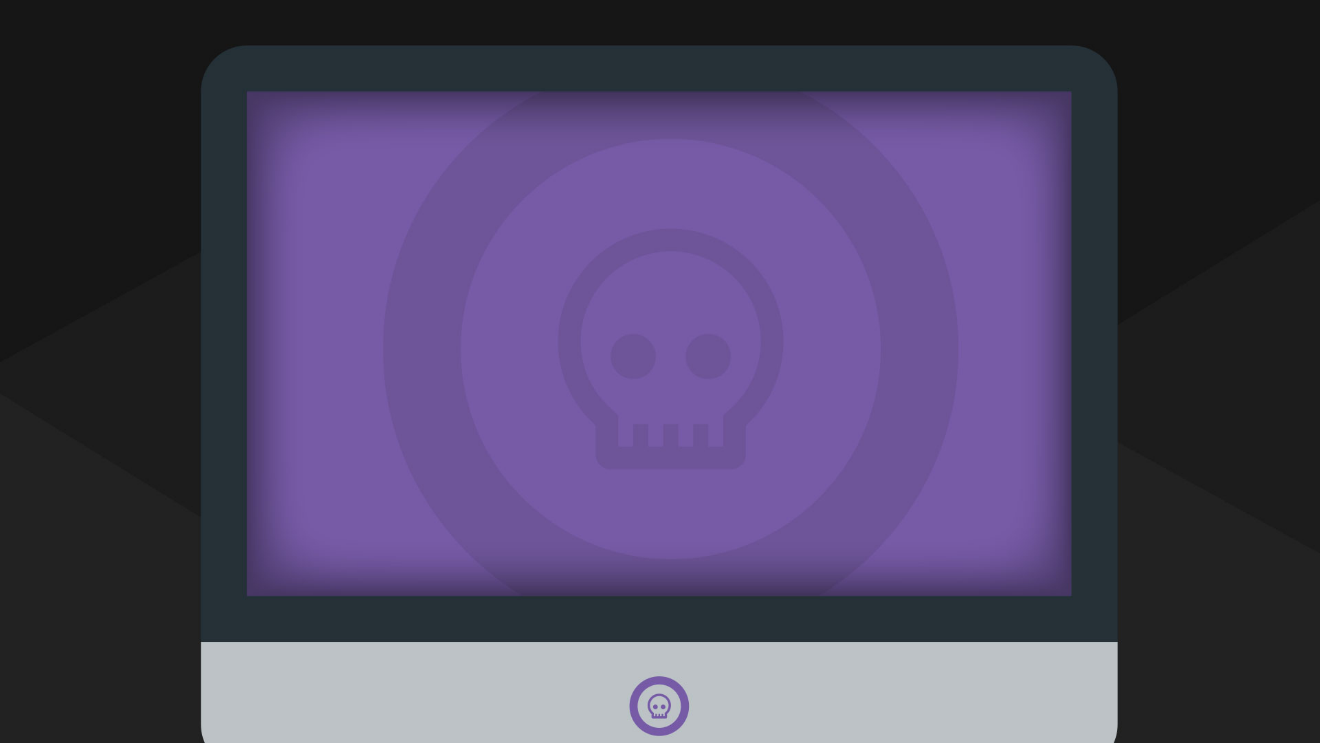
Nowadays, people use public Wi-Fi all the time in coffee shops, hotels, bars – the list goes on. However, if you do need to access the internet while away from your home or office,

You should be aware of the many threats to data security that lie in wait on public Wi-Fi.



Data sent over public Wi-Fi can be/cannot be intercepted by attackers.

Answer: can be



Any sensitive information that you send or receive while using these networks could be put at risk. True/Wrong

Answer: True

When looking to connect to public Wi-Fi, one of the most commons threat is public Wi-Fi networks.

These networks often have almost identical names to genuine networks and are designed to trick you into connecting.

Once connected, everything you do online can be seen by cyber criminals who monitor your activity waiting for any financial information or account credentials to be entered.

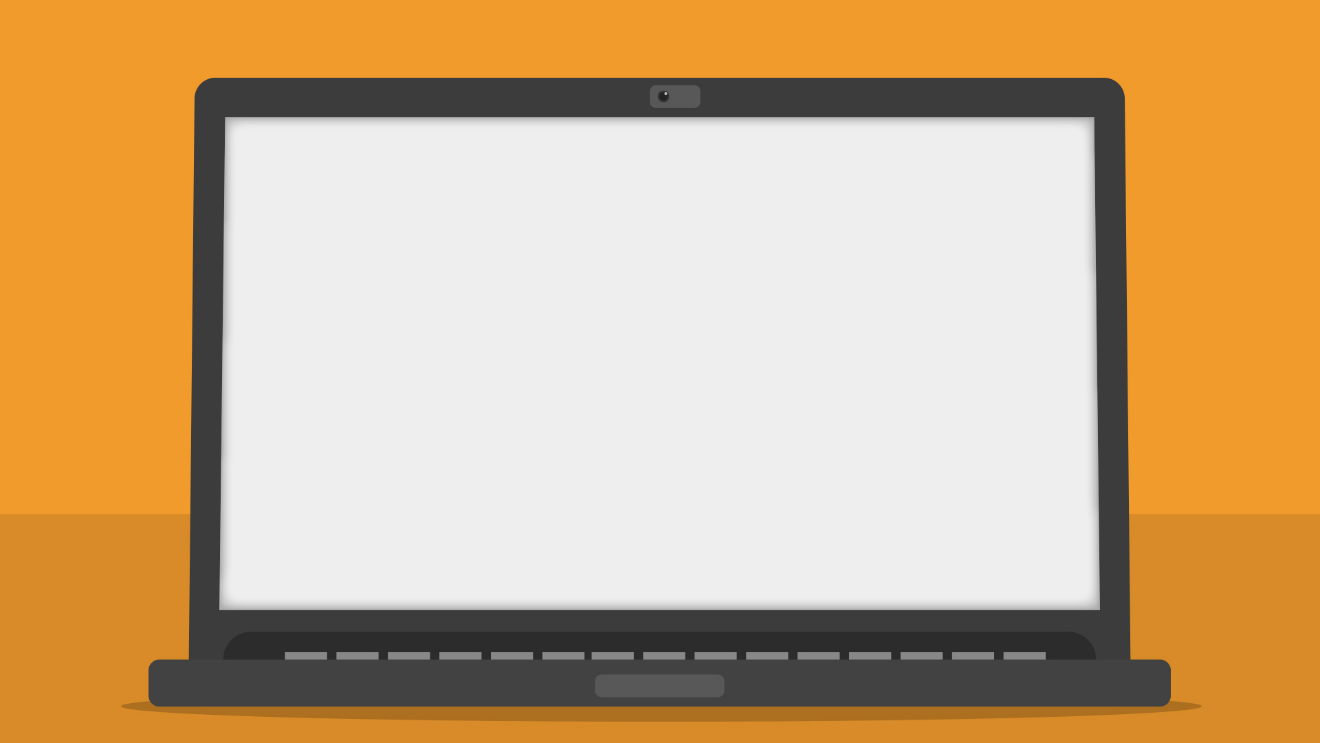
This is what is known as a\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Answer: Man-in-the-Middle-Attack.



It’s also worth remembering that \_\_\_\_\_\_\_\_\_\_\_\_\_\_ can also be used as a way of infecting your devices with malware.

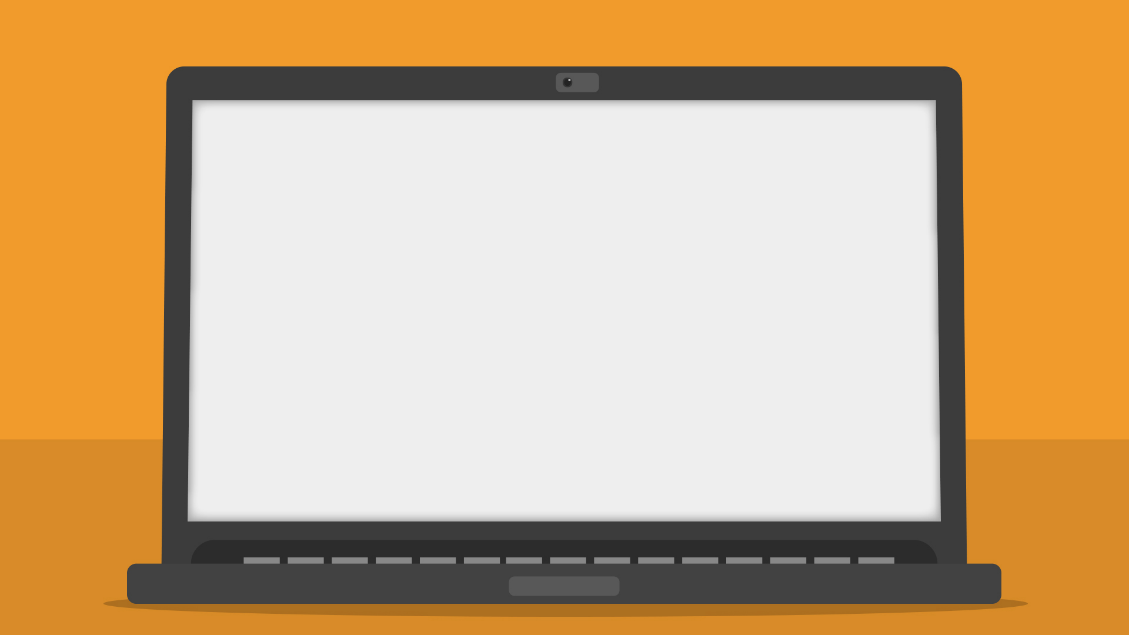
Answer: Public Wi-Fi



Cyber criminals can easily send across Trojans, viruses & other kinds of malicious software via a secure/unsecure Wi-Fi connection.

Answer: Unsecure

These are then able to cause damage to your computer and could also compromise any sensitive information stored within.



Fortunately, there are several steps you can take to stay safe when using Public Wi-Fi.

1: Verify Your Connection.

Make sure to check with a member of staff that you are connected to the correct public Wi-Fi.

Otherwise you could end up leaking sensitive information.



2. Use HTTPS.

You have probably seen the padlock before when typing a URL into your browser.

This is telling you that the site you are visiting is both sending and receiving information that is encrypted.

What is Encryption:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Answer: Encryption is incredibly useful if a malicious user is lurking on public Wi-Fi, just waiting for you to enter credit card numbers, passwords or account.



3. Turn off File Sharing.

Another thing you can do it to turn on/turn off any file sharing or AirDrop features before connecting to public Wi-Fi.

Answer: Turn off

If you do leave file sharing enabled, then attackers can access confidential information without you even realizing.



4. Be smart with Sensitive Data.

Unless it is essential, then you should refrain from logging into social media, financial or email accounts while connected to public Wi-Fi.

If you do need to check your bank account or send an email containing sensitive information, then it is worth doing it on your own device/private network.

Answer: own device



5. Use a VPN

By using a Virtual Private Network, also known as a VPN.

Even if an attacker positions themselves in the middle of your connection, your data will be intercepted/remain encrypted and impossible to read without a decryption key.

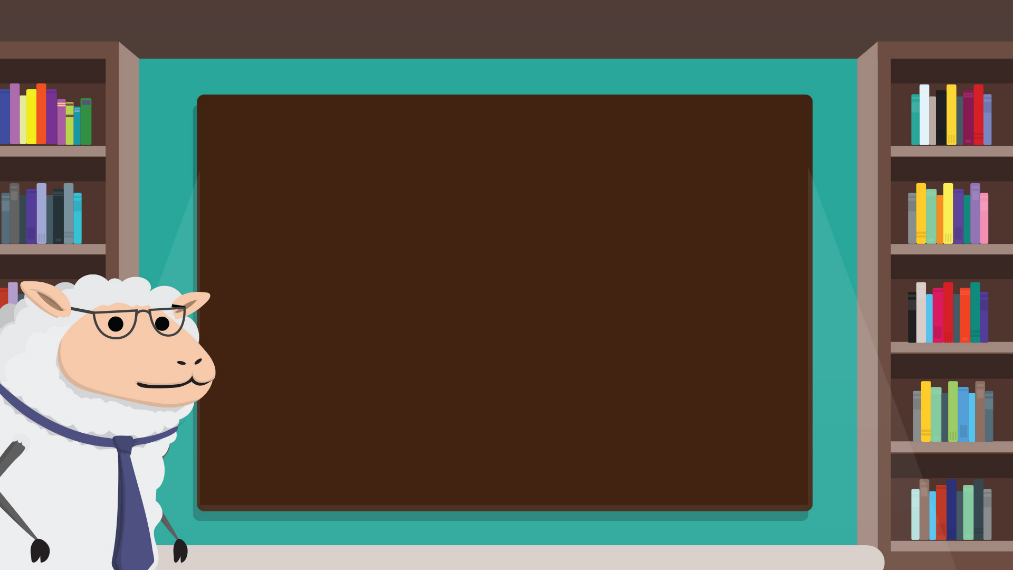
Answer: remain encrypted and impossible to read without a decryption key.

By following these steps, you will be able to benefit from all of the advantages that public Wi-Fi offers. While also being able to ensure that sensitive data remain secure.



Congratulations! You have completed the game and successfully answered all the questions.

In lesson 2 game, you have answered \_\_\_\_\_\_\_ questions correctly. The number of correct answers will be counted towards your final score. Thank you for your participation and enjoy the learning of iSecurity Platform!



Lesson 3 Game: Avoiding Password Peril

Staff are often unaware of the risks when creating passwords. The purpose of this text-based adventure game is to remind staff on the risks of choosing weak passwords and teach them to create strong passwords.

Please enter your name:

---------------------

电脑游戏画面

中度可信度描述已自动生成

Welcome,

----------------------! This game is intended to help you understand the risks when creating passwords. You can proceed the game by clicking the page. Each page will contain a scenario to guide you towards the next level. Once you start the game, you are required to fill in the blank, complete multiple-choice questions or true or false questions. After you are finished with the game, the number of correct answers will be shown in the end. They will be counted towards your final score. You can start your journey now!

电脑游戏画面

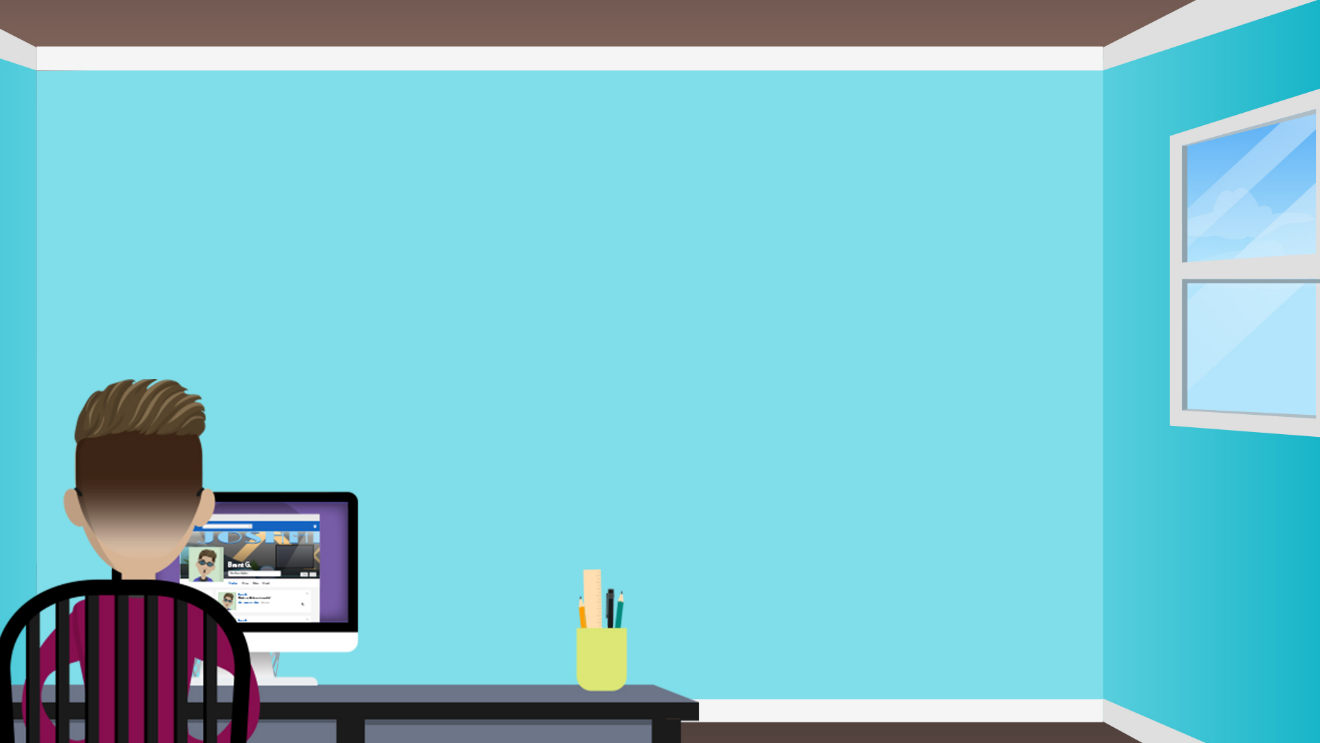
中度可信度描述已自动生成

This is a cyber criminal, Tom!

卡通人物

描述已自动生成

He is currently trying to hack into an unsuspecting social media manager (Amy’s) account for sensitive information.



However, it doesn’t take Tom to figure out that there are some passwords that are highly predictable and unfortunately common.

Abc123, qwerty, Password1, and many others are examples of this.

He frantically attempts each one of them, one after another into Amy’s password field for her email.

Wait! Looks like you may have underestimated Amy there, Tom.

Her email account remains secure.



Unless of course, Amy has left an alternate way of getting her password, on her public social media.

Oh no, Amy’s publicly shared obsession for his popstar is an easy assumption for what she might use as her password that anyone after a simple Google search of her name can see.

And now Tom is in.

Oh goodness, look at all that data that Tom is managed to come across!

表格

描述已自动生成

The filenames to those attachments – could they sound more attractive?

At the click of a button, these are downloaded, and company data has been compromised.



Being the social media manager, Amy runs other social media accounts for her company.

Let’s hope she hasn’t used the same password for them.

Looks like she did.

图形用户界面, 文本

描述已自动生成

So how could Amy have been more secure when creating her accounts?

As opposed to birthdays, pets, interest etc.

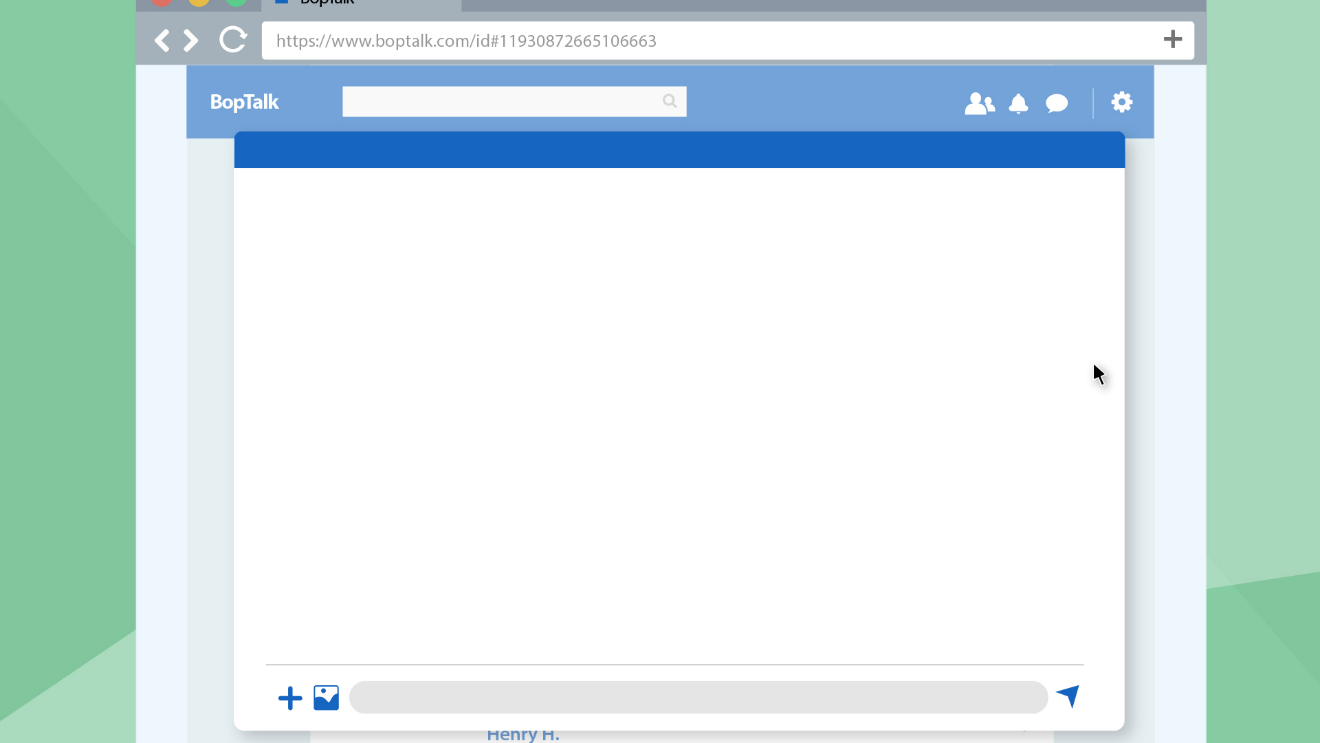
It’s better to have a password that isn’t directly linked to publicly obtainable information about yourself.

This time, Amy comes up with three random words.

Blue, Turkey, Hawaii, 66.

Ahh, now that’s a strong password.

Just avoid writing them down and displaying them.



Let’s see Tom try and guess that now.

Though Tom is clearly struggling a lot more than before, it’s not impossible for it to come by pure chance.

See, luckily though Amy also has two-factor authentication turned on.

文本

描述已自动生成

This means that instead of letting Tom get into her emails, the email service asks for a code from an authenticator app to confirm her identity.

Amy should take this opportunity to change her password.



Here, your knowledge of information security will be tested to check if you have fully understood the learning materials.

Staff should never use generic passwords like abc123 or P@sswordI.

True

False

Answer: True

Staff are allowed to use personal information like birthdays or pet names in passwords.

True

False

Answer: False

Staff are encouraged to writing down passwords or sharing them between colleagues.

True

False

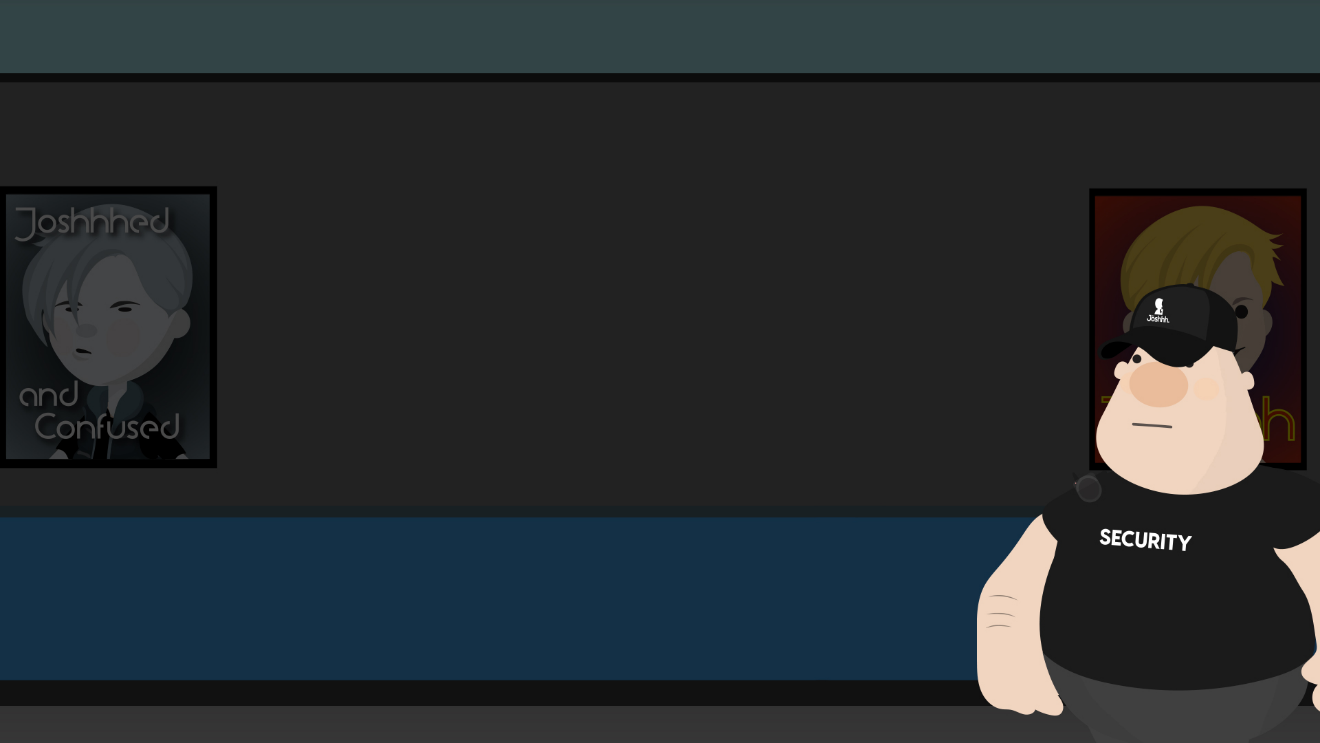
Answer: False

It is necessary to turn on two-factor authentication!

True

False

Answer: True



Congratulations! You have completed the game and successfully answered all the questions.

In lesson 3 game, you have answered \_\_\_\_\_\_\_ questions correctly. The number of correct answers will be counted towards your final score. Thank you for your participation and enjoy the learning of iSecurity Platform!

游戏机里面的人物

描述已自动生成