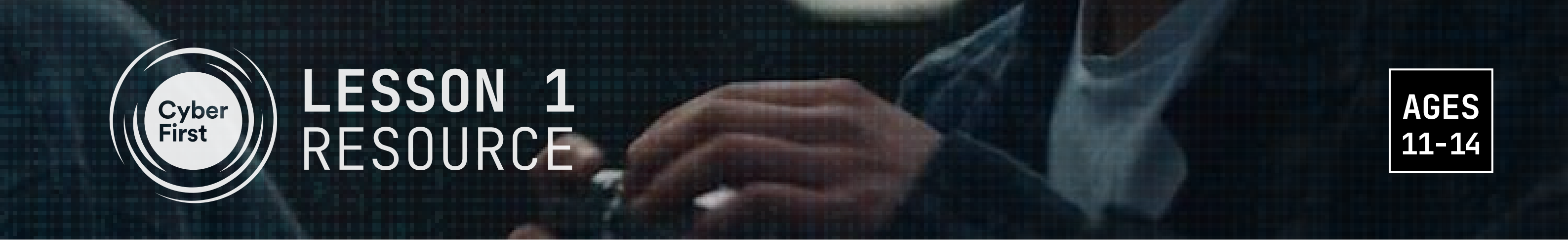


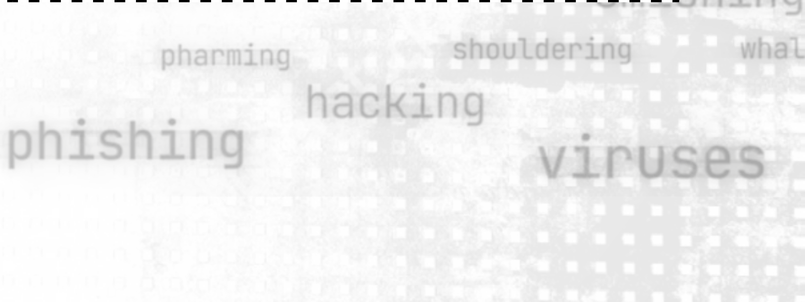
Cyber First

LESSON 1
RESOURCE

AGES
11-14

1: Risks and consequences

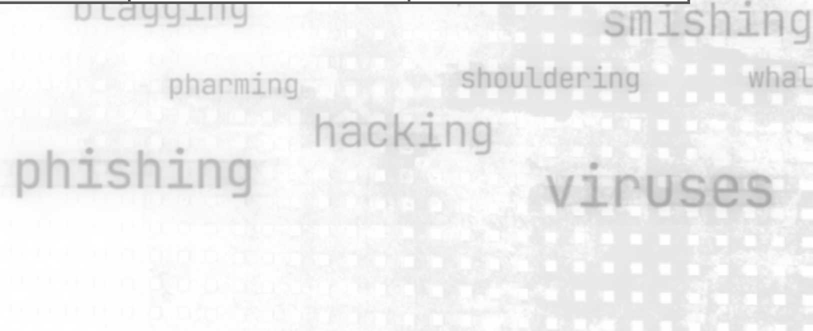
Olivia ignores a message on her laptop to update her operating system	Olivia may not have set up two-step verification
Luca’s account is hacked	Olivia uses the same password on multiple accounts
Luca’s password is compromised	Olivia’s account is hacked
Olivia makes a purchase through the unsafe weblink in a message from Luca’s account	Luca is locked out of his account
Luca has a password that is easy to guess	Olivia uses an old email address she hasn’t looked at in a while
Luca follows a link from social media to buy some headphones	Raheem shares his location data
The fake messages from Luca’s account include unsafe web links	Fake messages are sent to Raheem and Olivia from Luca’s account
Olivia’s email accounts are linked to her gaming accounts	Olivia follows an unsafe link sent from Luca’s account



National Cyber
Security Centre
a part of GCHQ

2: Social engineering?

Cyber security definitions:	Is this an example of social engineering? (tick)	Was this type of social engineering experienced in the film? (tick)
Viruses: Programs which can self-replicate and are designed to infect software programs or systems.		
Phishing: Untargeted, mass emails sent to many people, asking for sensitive information (such as bank details) or encouraging them to visit a fake website through a link. This could also be through social media messages. For example, someone might click on a fake advert and enter their details (credential harvesting).		
Blagging: When someone makes up a story to gain a person’s interest and engage them in communication, often via email.		
Malware: Malicious software - this includes viruses or any code or content that could have a negative impact on organisations or individuals.		
Pharming: When a user is redirected from a genuine website to a fake one because of malware on their device.		
Shouldering/Shoulder surfing: Looking at someone’s information over their shoulder, for example whilst they are entering a pin.		
Spear-phishing: A more targeted form of phishing, where the email is designed to look like it’s from a person the recipient knows and/or trusts.		
Malvertising: Using online advertising as a delivery method for malware.		
Smishing: Phishing via SMS - text messages are sent to users, asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.		
Ransomware: Malicious software that makes data or systems unusable until the victim makes a payment.		
Spyware: A type of malware that infects a PC or device and gathers information about the user, including online activity, usernames and passwords, payment information, and emails.		
Whaling: Highly targeted phishing attacks (which look like legitimate emails) that are aimed at senior executives.		

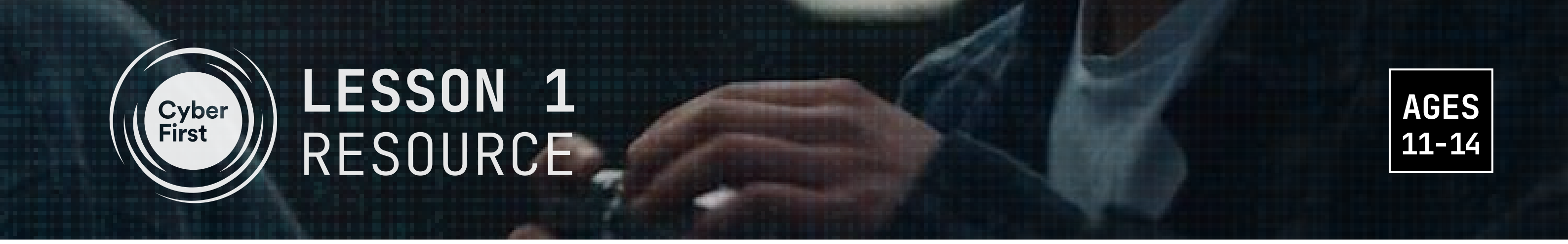


2b: Social engineering in the film

Which of the following types of social engineering were experienced by characters in the film?	✓
Phishing: Untargeted, mass emails sent to many people, asking for sensitive information (such as bank details) or encouraging them to visit a fake website. This could also be through social media messages. For example, someone might click on a fake advert and enter their details (credential harvesting).	
Blagging: When someone makes up a story to gain a person's interest, often via email.	
Pharming: When a user is redirected from a genuine website to a fake one because of malware on their device.	
Shouldering/Shoulder surfing: Looking at someone's information over their shoulder, for example whilst they are entering a pin.	
Spear-phishing: A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.	
Smishing: Phishing via SMS - text messages are sent to users, asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.	
Whaling: Highly targeted phishing attacks (which look like legitimate emails) that are aimed at senior executives.	

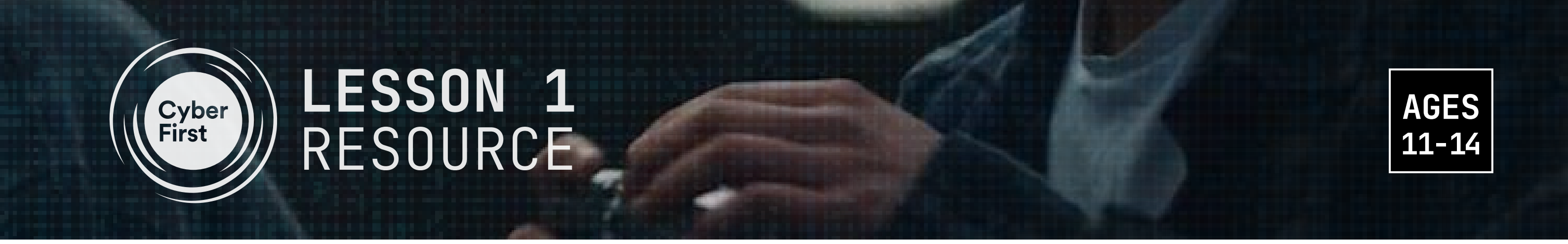
Circle the characters that were targeted and explain what happened below:

Circle the characters that were targeted and explain what happened below:		



2c: Social engineering in the film

Phishing	Programs which can self-replicate and are designed to infect software programs or systems.
Pharming	Untargeted, mass emails sent to many people, asking for sensitive information (such as bank details) or encouraging them to visit a fake website through a link. This could also be through social media messages. For example, someone might click on a fake advert and enter their details (credential harvesting).
Viruses	When someone makes up a story to gain a person’s interest and engage them in communication, often via email.
Malvertising	Malicious software - this includes viruses or any code or content that could have a negative impact on organisations or individuals.
Spyware	When a user is redirected from a genuine website to a fake one because of malware on their device.
Shouldering	Looking at someone’s information over their shoulder, for example whilst they are entering a pin.
Ransomware	A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.
Malware	Using online advertising as a delivery method for malware.
Blagging	Phishing via SMS - text messages are sent to users, asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.
Whaling	Malicious software that makes data or systems unusable until the victim makes a payment.
Smishing	A type of malware that infects a PC or device and gathers information about the user, including online activity, usernames and passwords, payment information, and emails.
Spear-phishing	Highly targeted phishing attacks (which look like legitimate emails) that are aimed at senior executives.



3: NCSC's Cyber Aware behaviours

1 **Use a strong and different password for email accounts**	Make sure that no other accounts use the same password as the email account. This means that if a cyber criminal stole the password for a less-important account, the email account would be safe. If they could access an email account, they could access private information, post emails and messages pretending to be the account holder, or reset other account passwords and get access to other online accounts.
2 **Create strong passwords for all accounts**	If passwords are easy to guess, it's easy to access accounts and personal information. Passwords should be long enough and strong enough to keep accounts safe. Three Random Words is one way you can make a long and strong password.
3 **Turn on 2-step verification (2SV)**	This is one of the most effective ways to protect accounts from cyber criminals. It means that a second piece of information, such as a code, or sometimes finger-print is needed to access an account, in addition to a password.
4 **Save passwords using a browser, or password manager**	This helps someone to use strong and different passwords across all of their accounts, because they don't have to remember them all.
5 **Back up data**	A backup is a copy of important data that's stored in a separate safe location, usually on the internet (known as cloud storage), or on removable media (such as USB stick, SD card, or external hard drive). It is a good idea to back up anything of value, as this means it can be replaced, should it be lost or stolen.
6 **Update devices**	Device updates include protection from viruses and other kinds of malware, and will often include improvements and new features. Applying security updates promptly helps to protect devices and accounts from cyber criminals and is one of the most important (and quickest) ways to keep safe online. It is also a good idea to turn on 'automatic updates' in a device's settings, if available.