Protecting against online fraud and scams

Age range: 14-16

BARCLAYS | LifeSkills

Definition of fraud and scams

- **Fraud:** when your account or card has been accessed, stolen or used without your knowledge. It can also be when a fraudster opens an account using your identity.
- **Scams:** are a type of fraud. When you're duped into making a payment by bank transfer for something you thought was genuine, like goods or services, which turn out to be fake. This can lead to a loss of money or services.

Match the term to the definition

Term	Definition
Money mule	A scam to access valuable personal details by using QR codes which ask you to download an attachment or follow a link to a website containing malware, which can collect secure information.
Online purchase scams	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Social engineering	Fraudsters send emails or text messages that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, due to an unauthorised payment.
Vishing	Someone advertising goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Phishing and smishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Quishing	Someone who is asked by a third party to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.

Definition of terms: answers

Term	Definition
Money mule	
Online purchase scams	
Social engineering	
Vishing	
Phishing and smishing	
Quishing	

Definition of terms: answers

Term	Definition
Money mule	Someone who is asked to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.
Online purchase scams	
Social engineering	
Vishing	
Phishing and smishing	
Quishing	

Definition of terms: answers

Term	Definition
Money mule	Someone who is asked to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.
Online purchase scams	Someone advertising goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	
Vishing	
Phishing and smishing	
Quishing	

Definition of terms: answers

Term	Definition
Money mule	Someone who is asked to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.
Online purchase scams	Someone advertising goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	
Phishing and smishing	
Quishing	

Definition of terms: answers

Term	Definition
Money mule	Someone who is asked to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.
Online purchase scams	Someone advertising goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing and smishing	
Quishing	

Definition of terms: answers

Term	Definition
Money mule	Someone who is asked to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.
Online purchase scams	Someone advertising goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing and smishing	Fraudsters send emails or text messages that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, due to an unauthorised payment.
Quishing	

Definition of terms: answers

Term	Definition
Money mule	Someone who is asked to receive money into their bank account and transfer it onto another account, or allows another person to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering. This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.
Online purchase scams	Someone advertising goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing and smishing	Fraudsters send emails or text messages that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, due to an unauthorised payment.
Quishing	A scam to access valuable personal details by using QR codes which ask you to download an attachment or follow a link to a website containing malware, which can collect secure information.

Financial fraud, scams and identity theft in action

Case study 1

"Jake was keen to get tickets for a football match which had sold out. He found some advertised on a social media app for much cheaper than the original price, and paid for them via bank transfer. Jake was sent a confirmation from the seller that the tickets would be emailed to him within 10 days.

Unfortunately, the tickets never arrived and when he made calls to the seller they were ignored. Even though he tried to report the seller, there was very little he could do to get his money back."

Financial fraud, scams and identity theft in action

Case study 2

"Tom received a text message to say that his bank account details had been used by someone else to download lots of apps. To get a refund, Tom was asked to click on a link and enter his bank details and the three digit security code on his debit card into a form online; he was told that this refund would appear in his account within 5-10 days.

The following day, when Tom checked his bank balance using his mobile banking app, he saw that a large sum of money had been withdrawn from his account."

Summary: student sheet

Top tips for staying safe online

1. Check which personal information is public on your social media accounts, e.g. your birthday, hometown, pet names, holiday dates, job title. Fraudsters can use this information to steal your identity and apply for bank accounts or buy products in your name.
2. Be wary if you see encouragement to click on an unknown link – if you're not sure, visit the organisation's website directly.
3. Never share your PIN, bank details or passwords with anyone who contacts you through text, email, phone or in person, and don't write them down. Never let anyone else access your account.
4. Remember that letting someone else use your bank account is a potentially serious crime which could damage your financial future, so take time to think it through and talk to an adult you trust.
5. Phone organisations directly from the number listed on their website to verify who is contacting you.
6. Password protect your devices using random words and include symbols, numbers and capitals. Set passwords to be at least 10 characters long and don't use the same passwords for different accounts.
7. Limit your online activity when using open public Wi-Fi connections, including logging on to your email, online banking and online shopping.
8. Hover over links before clicking on them to reveal the web address destination. Install anti-virus software on your laptop and any other personal devices and keep it up to date.
9. If you have any concerns, share them with someone you trust, whether it's a parent, tutor or friend.