



Spotting online shopping scams

Age range: 16-19

 **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

3

Term	Definition
Money mule	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.
Online purchase scams	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.
Social engineering	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.
Vishing	A scam where the fraudster goes to great lengths to gain your trust and convince you that you are both in a genuine relationship. They will often build a relationship over a long period of time, expressing serious feelings for you quite quickly, love bombing you to make your connection seem more special. They will frequently deny requests for video chat as their profile image may differ from the person you are actually speaking to. They use persuasive language to make requests for money to pay for things like transport or emergency medical care.
Phishing and smishing	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.
Quishing	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.
Romance scams	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.

Definition of terms: answers

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

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	
Romance scams	

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	
Romance scams	

Definition of terms: answers

Term	Definition
Money mule	<p>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.</p> <p>This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.</p>
Online purchase scams	<p>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.</p>
Social engineering	<p>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.</p>
Vishing	
Phishing and smishing	
Quishing	
Romance scams	

Definition of terms: answers

Term	Definition
Money mule	<p>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.</p> <p>This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.</p>
Online purchase scams	<p>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.</p>
Social engineering	<p>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.</p>
Vishing	<p>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.</p>
Phishing and smishing	
Quishing	
Romance scams	

Definition of terms: answers

Term	Definition
Money mule	<p>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.</p> <p>This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.</p>
Online purchase scams	<p>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.</p>
Social engineering	<p>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.</p>
Vishing	<p>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.</p>
Phishing and smishing	<p>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.</p>
Quishing	
Romance scams	

Definition of terms: answers

4

Term	Definition
Money mule	<p>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.</p> <p>This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.</p>
Online purchase scams	<p>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.</p>
Social engineering	<p>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.</p>
Vishing	<p>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.</p>
Phishing and smishing	<p>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.</p>
Quishing	<p>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.</p>
Romance scams	

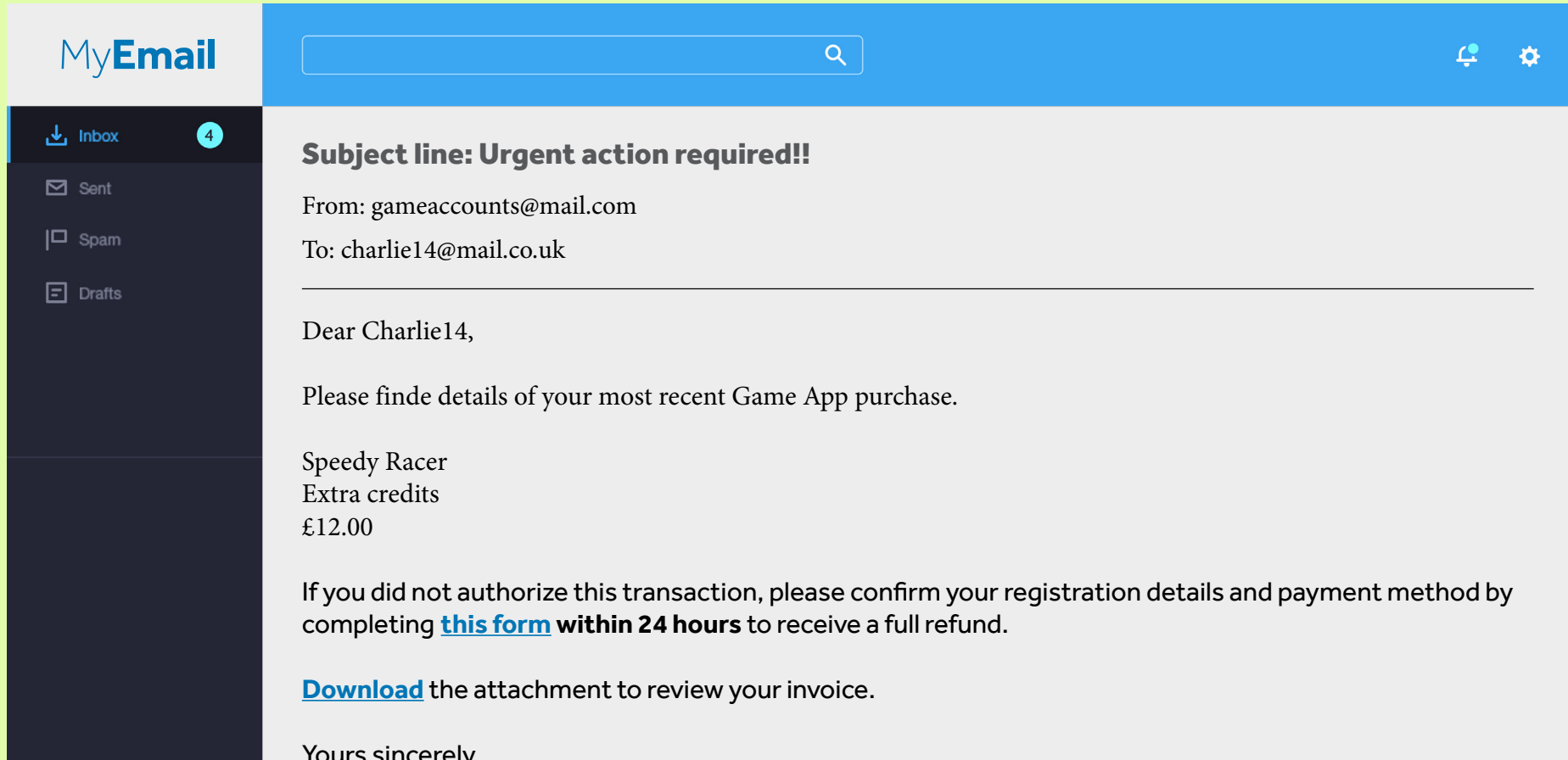
Definition of terms: answers

Term	Definition
Money mule	<p>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.</p> <p>This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.</p>
Online purchase scams	<p>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.</p>
Social engineering	<p>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.</p>
Vishing	<p>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.</p>
Phishing and smishing	<p>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.</p>
Quishing	<p>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.</p>
Romance scams	<p>A scam where the fraudster goes to great lengths to gain your trust and convince you that you are both in a genuine relationship. They will often build a relationship over a long period of time, expressing serious feelings for you quite quickly, love bombing you to make your connection seem more special. They will frequently deny requests for video chat as their profile image may differ from the person you are actually speaking to. They use persuasive language to make requests for money to pay for things like transport or emergency medical care.</p>

Spot the faker

5

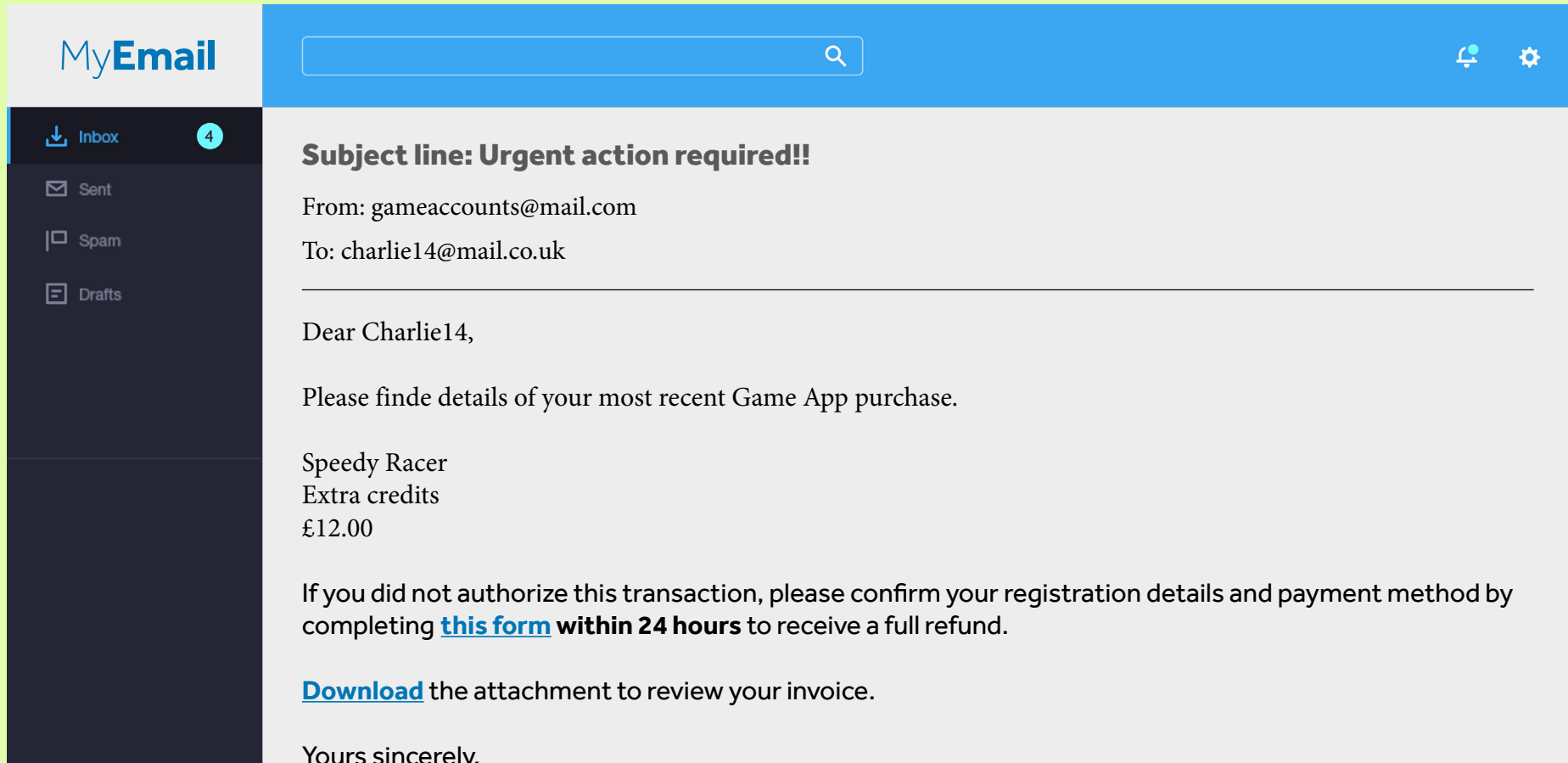
This email may be from a scammer. Can you identify the suspicious signs?



Imagery or design that looks familiar but doesn't feel right

6

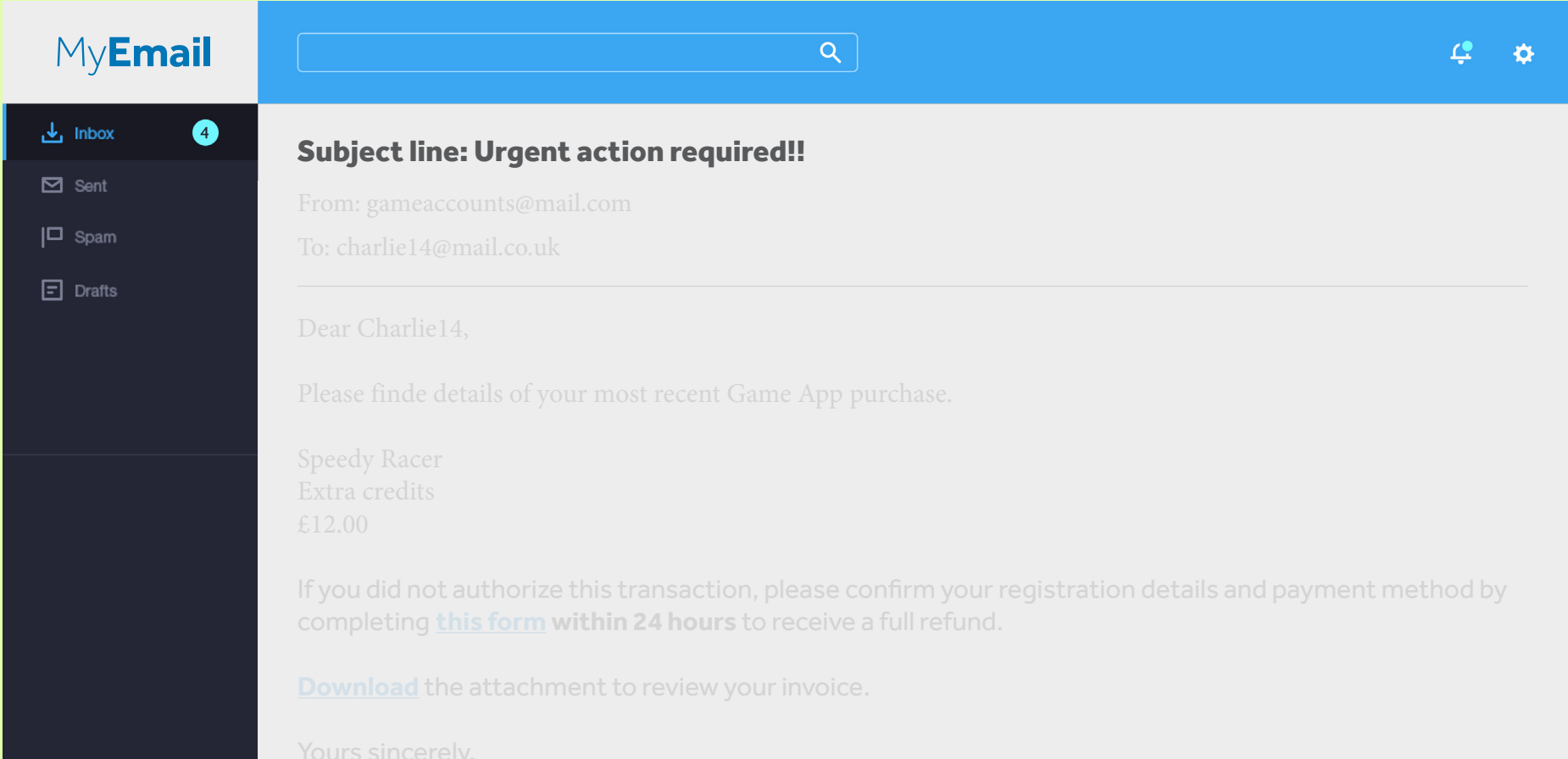
Email design, fonts or imagery that don't look as you'd expect can be a sign that it's not from a genuine sender.



Message subject line

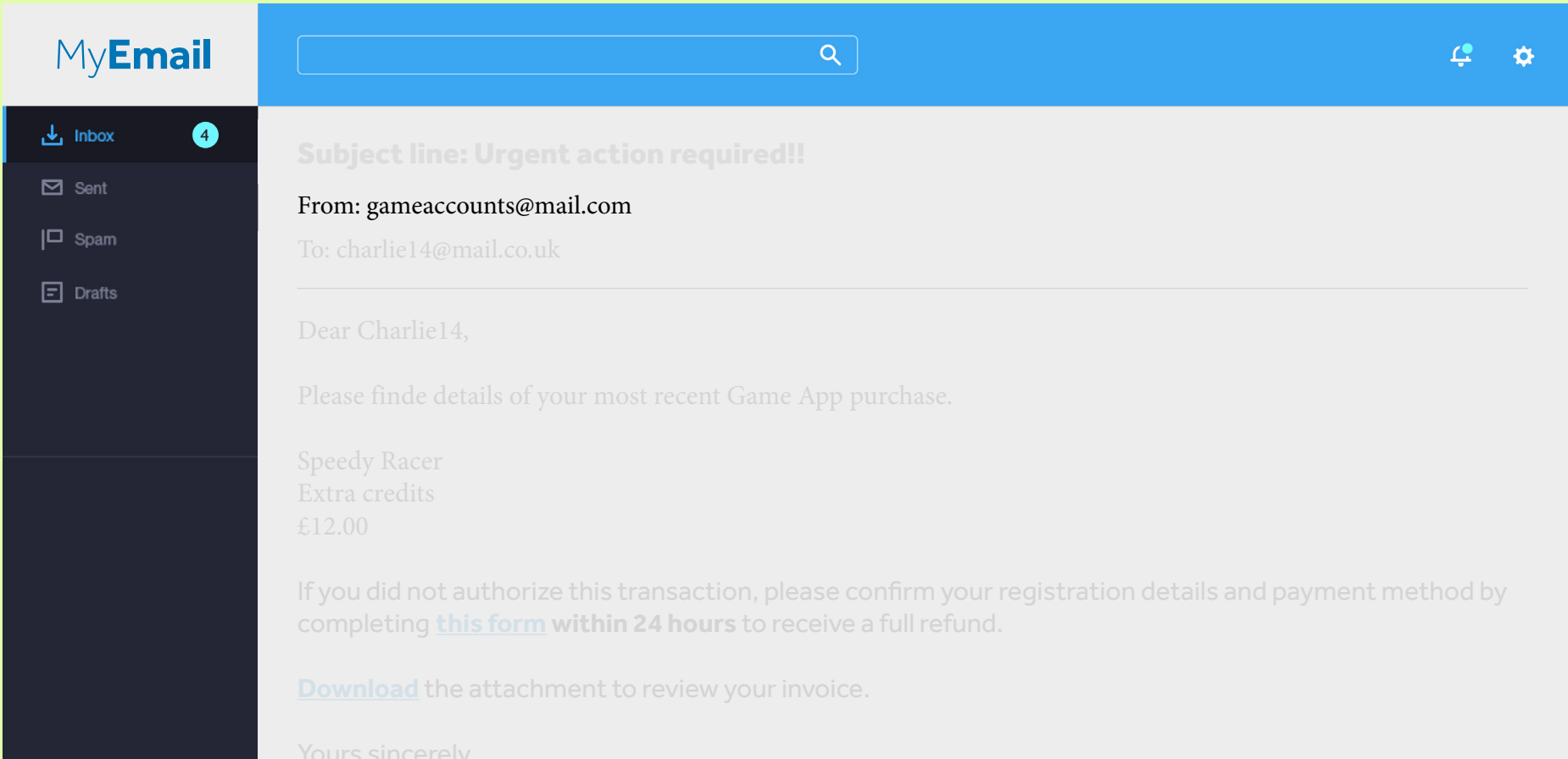
7

Be suspicious of urgent requests or something that sounds too good to be true. Fraudsters often use these tactics to encourage a quick response.



Sender

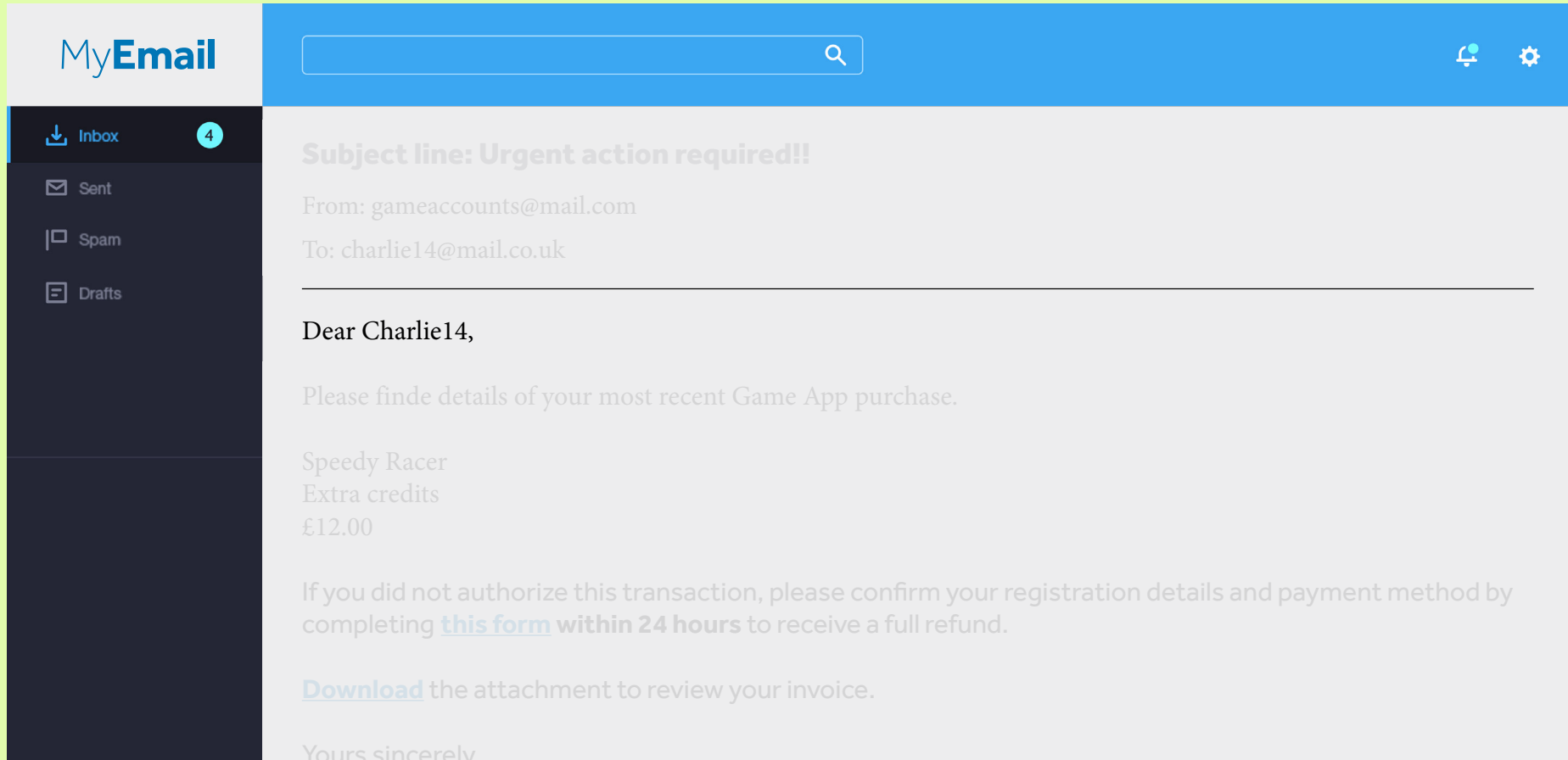
Look at the sender to see if the email address is suspicious. For example, it might not match who the sender says they are or it may be from an email address like Google or Yahoo which anyone can create instead of a business one.



'To' line

9

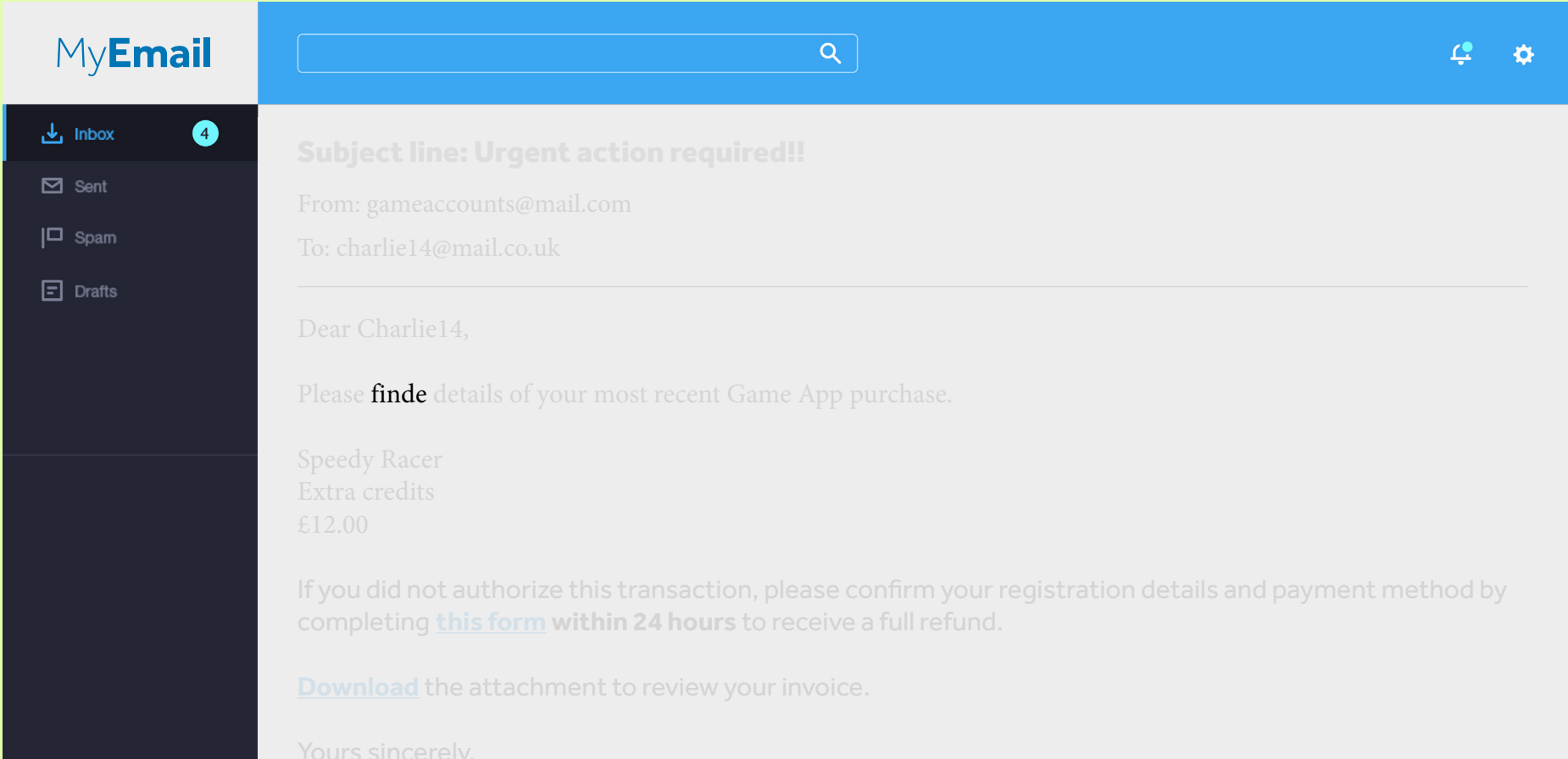
Watch out for emails that refer to you in an unusual way, such as the first part of your email address. A trustworthy organisation is more likely to use your full name.



Poor grammar/mistakes

10

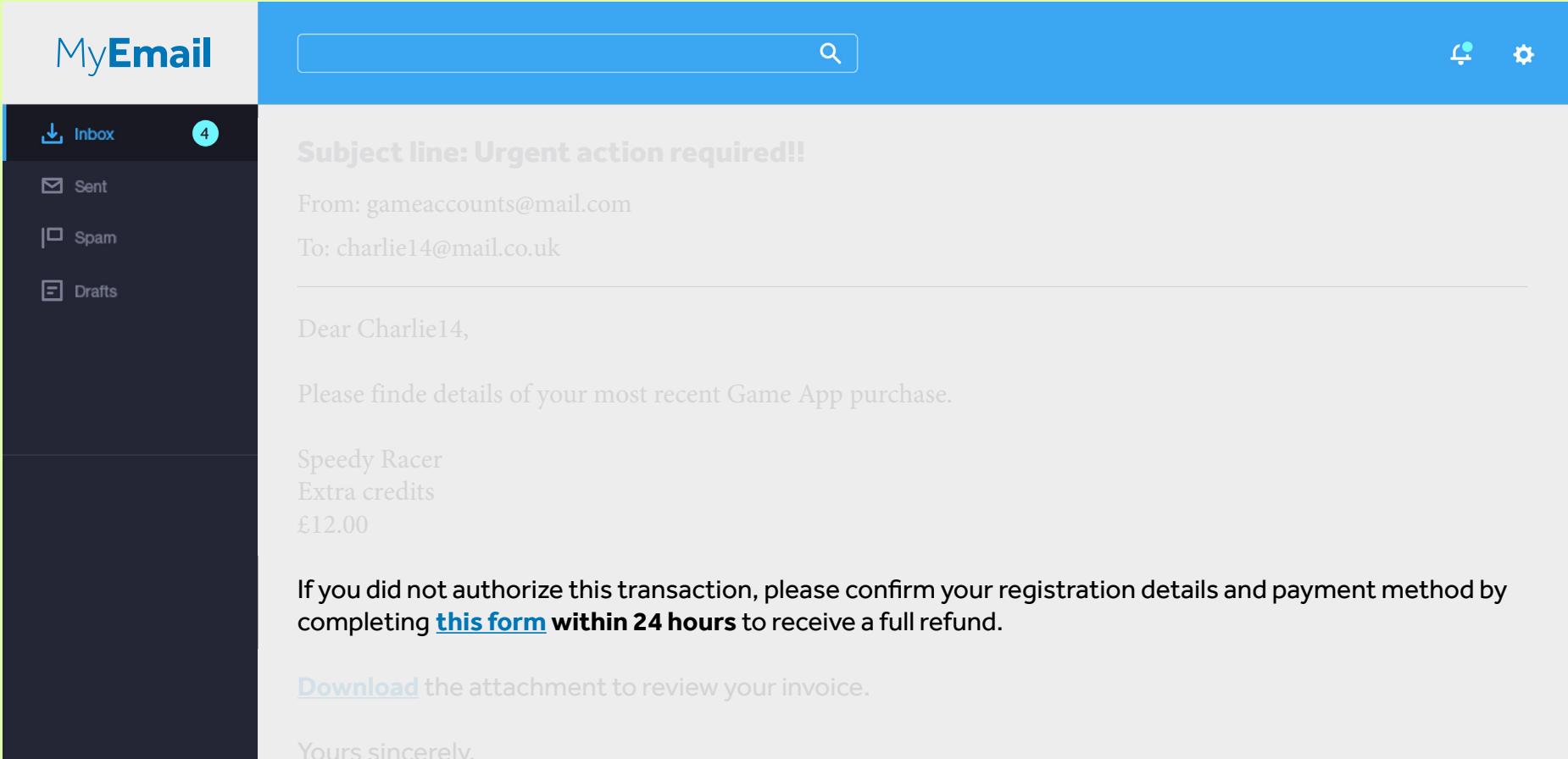
Poor grammar, unusual style and mistakes in the wording of the message can be a sign that it is not from a genuine sender.



Request for personal details/completing a form

11

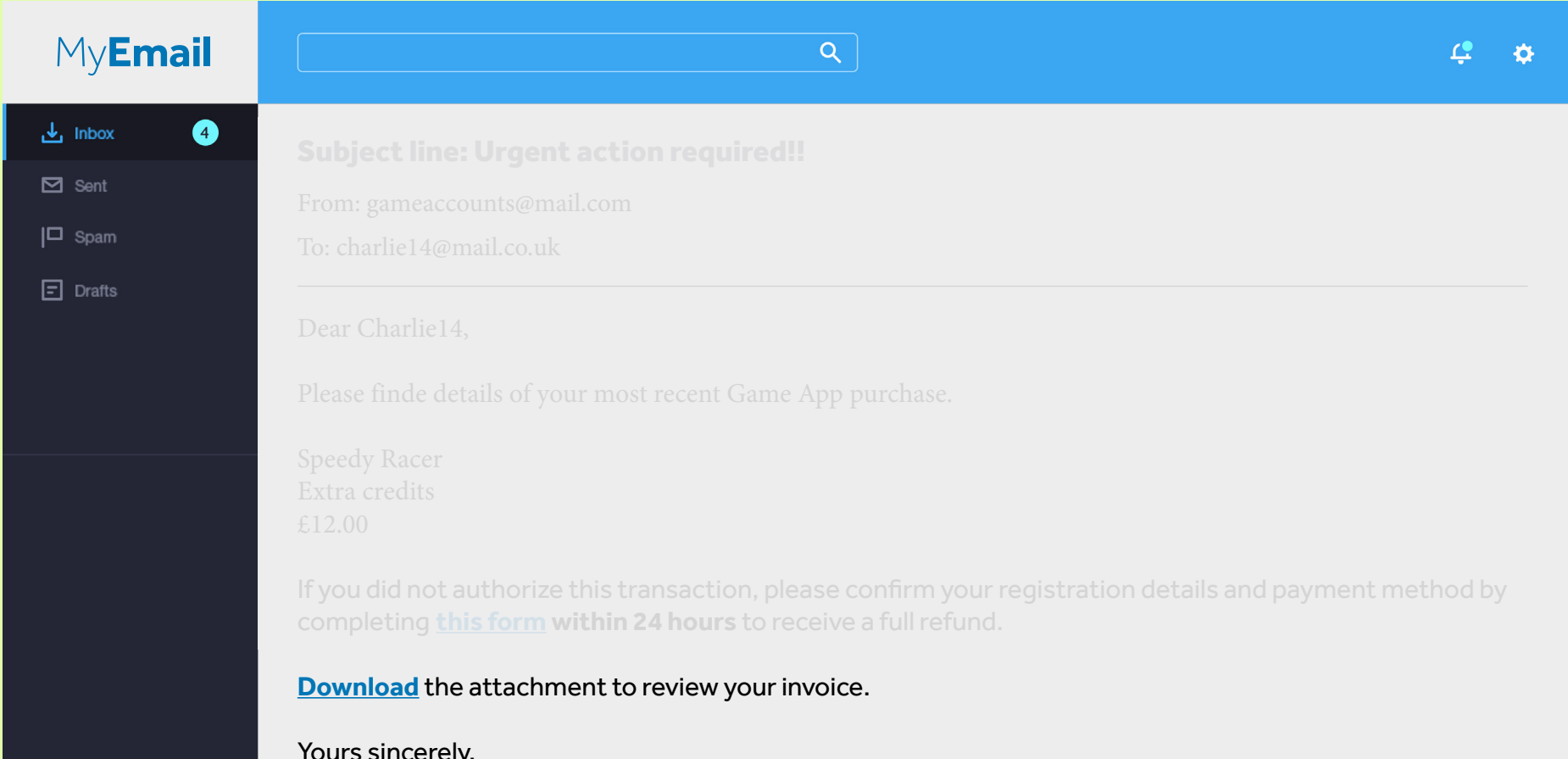
Trustworthy organisations will never request that you provide your PIN, password, or online banking login details, or ask you to transfer money to another account.



Hyperlink to follow or attachment to download

12

Never open attachments or click on a link from someone you don't know or weren't expecting. You might be directed to a fake website where your login and personal details are requested and stolen, or your device could be infected by a virus. Hover over hyperlinks without clicking to display the destination and evaluate whether it looks real.



Financial fraud, scams and identity theft in action

Case study – House hunting

"Mia has been looking online for flats to move into with two friends. She has been having a hard time on rental and property websites as properties are let out very quickly. She finds a three-bedroom flat in a housing group on a social media app, and enquires about its availability. The landlord asks Mia to transfer one week's deposit to hold the property. Mia transfers the money via bank transfer. Mia doesn't really want to do this but she's so desperate for this flat she transfers the money via bank transfer.

However, after she transfers the money she doesn't hear from the landlord again."



Top tips for protecting yourself from fraud, scams and identity theft

14

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. Beware of offers that sound 'too good to be true', particularly if they are offering higher return on investment in foreign currency, stocks and shares or cryptocurrencies.
4. 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.
5. 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.
6. Phone organisations directly from the number listed on their website to verify who is contacting you.
7. 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.
8. Limit your online activity when using open public Wi-Fi connections, including logging on to your email, online banking and online shopping.
9. Hover over links before clicking on them to reveal the web address destination.
10. Install anti-virus software on your laptop and any other personal devices and keep it up to date.
11. If you are a victim of fraud, you should freeze your card immediately and contact your bank. From here, you should make a list of the fraudulent transactions and learn from what has happened. It is important to stay vigilant.
12. If you have any concerns, share them with someone you trust, whether it's a parent, tutor or friend.