

### Fake emails using AI technology

Fake emails and text messages will attempt to prompt you into following a phishing link that will ask for personal and/or financial information. This is typically done by impersonating well known brands and asking you to update your account information or to follow a link to receive a prize.

With generative Artificial intelligence commonly known as AI, criminals are able to use tools such as ChatGPT, to create more convincing messages, free from the poor spelling and grammar we have always relied on to spot scams.

Therefore, here some tips to help you identify a scam –

- Most genuine companies address you by your name.
- Messages asking for personal and financial data should be treated with caution.
- Be wary of messages with attachments, as most companies never include these
   and this is how scammers spread malware.
- All phishing messages contain links. So wherever possible avoid clicking on links and if unsure contact the company by phone.
- Brands will use their official email addresses, so always check the sender's address
  on emails.
- Always check the number that texts are sent from although numbers can be spoofed (impersonated), a seemingly random number is always a red flag.
- Scammers want to push you to act quickly, so be wary of a sense of urgency.
- Check the branding for blurred or pixelated images that do not use the company's latest brand colours.

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at <a href="www.actionfraud.police.uk">www.actionfraud.police.uk</a> or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police













### **Courier Fraud Alert**

Last week we received reports of Courier Fraud in Sevenoaks, Maidstone, Gillingham, Dartford and Tenterden.





This scam works by residents receiving a phone call from criminals impersonating the Police or their bank. They will state that someone has used their card and they need to collect their bank cards via courier as evidence. They may also ask for your bank details to assist with an ongoing investigation or tell you that they have a family member in custody.

All these calls are scams by criminals trying to get your financial details. If you get a call like this and then a courier arrives at your property ring 999.

Additionally, the Police will NEVER telephone and ask your bank card and pin number to be collected by a courier or withdraw cash or buy gold to assist in an investigation.

Always check the dialling tone after your call to ensure scammers are not still on the phone and use another telephone if possible or call a trusted friend first to ensure that the line has been disconnected.

Watch - Courier Fraud Warning: Stay Wise, Don't Compromise (youtube.com)



## **Preventing fraud**

Together, let's stop scammers.



Remember, ABC:



















### Aldi Fake email offering an unbelievable free £200 Gift Card!!!!!

Be on the lookout for fake emails impersonating Aldi offering a free £200 gift card and all you must do is click the link and answer a few simple questions, it's a SCAM. The link will take you to a realistic looking website under the control of the criminals, where they will steal your personal and financial data.

I received this earlier today and thought I would share this one with you all. One of the obvious signs is the sending email address which is not an official Aldi email. Additionally, it does not address me by name, as this scam email is sent to thousands of people at the same time. Finally, the £ sign is behind the 200 under where it says, "we value your feedback (see below)."



Together, let's stop scammers.



Remember, ABC:



never **A**ssume



<u>never</u> Believe



always Confirm

--- Original Message From: info+eumxpfmck@bibliotecadaterra.com Sent: Friday, August 23rd 2024, 09:29 Subject: ff£200 Aldi gift card Exclusive Rewards For You

#### £200 Aldi gift card Exclusive Rewards For You



We Value Your Feedback!

You have been selected as one of the lucky few for a unique opportunity to receive a ALDI 200£ Giftcard!

To claim, Simply answer a few quick questions regarding you experience with ALDI.

You can report these by forwarding to <a href="mailto:report@phishing.gov.uk">report@phishing.gov.uk</a>

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police











### **Romance Scams**

Criminals are experts at impersonating people. They spend hours researching you for their scams, especially when committing romance fraud.

Romance fraud involves people being tricked into sending money to criminals who go to great lengths to gain their trust and convince them that they are in a genuine relationship. They use language to manipulate, persuade and exploit so that requests for money do not raise alarm bells. These requests might be highly emotive, such as criminals claiming they need money for emergency medical care, or to pay for transport costs to visit the victim if they are overseas. Scammers will often build a relationship with their victims over time before asking for money.

How can you remain safe?

- Be suspicious of any requests for money from someone you have never met in person, particularly if you have only recently met online.
- Speak to your family or friends to get advice.
- Profile photos may not be genuine, do your research first. Performing a reverse image search on a search engine can find photos that have been taken from somewhere or someone, else.

## Preventing fraud

Together, let's stop scammers.



Remember, ABC:







No matter how long you have been speaking to someone online and how much you think you trust them, if you have not met them in person, is important that you do not:



- Send them any money.
- Allow them access to your bank account.
- Transfer money on their behalf.
- Take a loan out for them.
- Provide copies of your personal documents such as passports or driving licenses
- Invest your own money on their behalf or on their advice.
- Purchase and send the codes on gift cards from Amazon or iTunes.
- Agree to receive and/or send parcels on their behalf (laptops, mobile phones etc).

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police











### **Online shopping Fraud**

Getting ready for the new term and purchasing those new uniforms etc? Well beware of online shopping fraud, which is one of the largest reported frauds targeting the public.

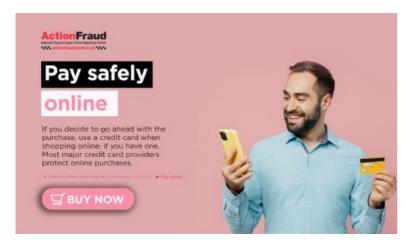
Always do your research -

Use a credit card when shopping online. Most major credit card providers will protect online purchases against fraud.

For more top tips on how to shop safely online, visit - <u>Shopping online securely |</u> Action Fraud

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at <a href="www.actionfraud.police.uk">www.actionfraud.police.uk</a> or call 0300 123 2040.

For further information about Fraud, visit our website at <a href="Advice about fraud">Advice about fraud</a> <a href="Kent Police">Kent Police</a>



## **Preventing fraud**

Together, let's stop scammers.



Remember, ABC:













