



ONLINE SCAMS

MORE MONEY WAS LOST TO ONLINE SCAMS LAST YEAR THAN EVER BEFORE

The criminal's aim is to obtain financial information to enable them to empty bank accounts through money transfers or the purchase of goods and services.

The most common scams arrive by email. Here's what to look out for...

- General greeting like 'dear customer'
- Sense of urgency, ie 'act now or your account will be closed'
- Prominent website links can be forged to look similar to the proper address. One different letter means a different website
- Request for personal information such as user name, password or bank details
- Poor spelling and grammar
- Text is contained within an image
- You weren't expecting an email from the company that appears to have sent it



WHAT TO DO IF YOU RECEIVE A SCAM EMAIL

- Do not reply or contact the sender
- Do not click on links or open attachments
- If you have already clicked on a link and opened a website, do not give out any personal information
- Delete it!

SOME OF THE MOST COMMON SCAMS

- Computer viruses
- Fake websites
- Online shopping
- Phishing emails
- Relationship scams

PROTECT YOURSELF

- Never give anyone access to your computer
- Microsoft or someone on their behalf will never call you
- If you need technical help, always call or email your internet service provider's support line or talk to a computer repair company locally
- Never share passwords or pin numbers
- If you provide personal information (login, sign up or register) check there's a padlock symbol in the browser window frame (next to the web address). Make sure the padlock is not only on the page itself.



IF YOU THINK YOU HAVE BEEN A VICTIM

- Contact your bank to stop any payments being taken
- If you have lost money, it is possible your Credit Card Company or contents insurance may cover the loss
- Get your computer checked for any malware or Trojans that may have been installed
- Report it to the Citizens Advice consumer service on 03454 04 05 06, or tell the Police.

kent.gov.uk/tradingstandards

- Update your browser to the latest version
- Use up-to-date security software
- Roll your mouse over links to reveal the actual sender



TRADING STANDARDS