

The Essential Guide to Online Safety



This short course will give you a few tips on how to stay safe online



This is serious



ONS:

"Fraud is now the most common crime in England and Wales. It costs the UK **£137bn** a year..."

"There were **4.5 million** reported offences of Identity Theft in 2022"



National Crime Agency:

"...we think that **fewer than 20 per cent** of incidents of fraud are actually reported"

House of Commons Justice Committee:

"Just **2 per cent of police funding** is dedicated to combating fraud despite it making up **40 per cent of reported crimes** in England and Wales. More than half of all fraud is believed to be carried out over the internet"



Victims Commissioner:

"**4.6 million people** are affected by fraud each year and around **700,000** will go on to suffer profoundly"



National Audit Office:

"There is an **86%** year-on-year increase in online fraud"



HM Inspector of Constabulary:

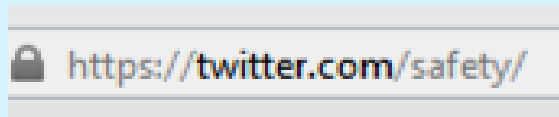
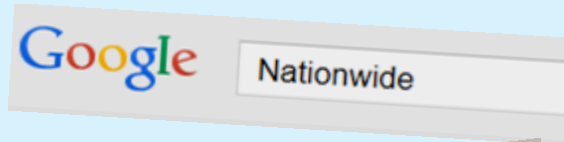
"Kent Police received **12,000 reports** of fraud from Action Fraud in 2022. This resulted in **20 prosecutions**"



The Essential Guide to Online Safety

Subjects we will cover are:

Passwords
Internet Banking
Phishing
Forged Websites
Genuine websites
Using Money Online
Secure Websites
Logging Out
Email Scams
Security Software



Passwords

You will have passwords for everything
(Bank accounts, Amazon,
Social Media, PayPal, email etc)

**What makes a good
password?**

You can recall it exactly
No-one else can guess it



Passwords

Weak passwords:

letmein, 0000, password, 123456

Lower case (small letters) only
No mix of numbers & letters
Few characters
Easy to guess





Passwords



Strong password:

LondoN2018, 19Evelyn82

Mix of lower & upper case and a few numbers
More characters. Still easy to remember

Tp4ZrT5q1i9s3z5c2iD

Great password but difficult to remember!

Passwords

Even stronger passwords:

Use 'odd' character from the keyboard –

! " £ \$ % ^ & * € and so on.

These **dramatically** improve password strength

Passwords

Good Passwords – that you remember:

Use an acronym that means something to you. Example:

My daughter's birth date is 13 April 1982

Can become: **Md'sbd13April82**

or

Use three (or more) words. Example:

Fruitbowl.Wardrobe.Printer

Passwords

Don't use:

Something that could easily be guessed

(Own / partners / child's / grandchild's name/ favourite football team, street where you live, pet's name etc)

Do use:

Something that could NOT be easily guessed:

(Mother's place of birth, partner's middle name, father's first name)

Consider:

A Password Manager. 'Lastpass'; 'Dashlane'; 'Roboform' etc

(Search for 'password manager')


Passwords

Good to use different passwords for different places –
but difficult to remember them all

Use a few passwords

Use more complex passwords for important websites

(It won't matter if your utility company and the site you use for sending e-cards have
the same password.)

The  recommend that you do **NOT** change
your password regularly

(Only change it if you think it's been compromised)

Passwords

If you write them down,
don't make it obvious!



Write them in a way (and in a
place) that no-one will
understand what they are



Passwords

**Don't forget your
mobile phone!**

Most are purchased with
no password set

(Use fingerprint / facial recognition if available)



Passwords

Whatever password you choose,
check out how good it is at
passwordmonster.com

A password based on your
grandson's name and birth
year doesn't take long to
break

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☒

George+2018

Very Weak

11 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:
18.09 seconds

Fruitbowl.Wardrobe.Printer

Very Strong

s containing:

Lower case

Upper case

Numbers

Time to crack your password:
4 million years

These
passwords
take a bit
longer

Md'sbd13April82

Very Strong

containing:

Lower case

Upper case

Number

Time to crack your password:
29 million years

Internet Banking

Co-operative
Online Banking



Santander
Online Banking





Bank Accounts



Have excellent security

Banks give an online guarantee

To access your online account you'll need a variety of details: Customer number, Date of Birth, a one-time-code and a pass number....

(Two Factor Authentication)



Bank Accounts

The pass number

You have to enter parts of it. Perhaps the 2nd, 3rd & 6th numbers

(Tomorrow it will be the 2nd, 1st & 5th)



Enter the 2nd, 3rd and 6th digits from your passnumber

<input type="text"/>	<input type="text" value="-"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="-"/>	<input type="text" value="v"/>
	2nd	3rd			6th	

[Forgotten your passnumber?](#)

Continue

Bank Accounts

**Bank security is probably
perfect**



So - how are you tricked into
letting them in?

Phishing

You might be sent a ***phishing*** email like this:



Dear Customer,

Your account has been placed on restricted status. Restricted accounts continue to receive payments, but they are limited in their ability to send or withdraw funds.

To lift this restriction, you need to confirm your identity. All restricted accounts have their billing information unconfirmed. To initiate the confirmation process, [Click Here](#)

Phishing

Or one like this:

Dear **Western Union** valued customer,

You received this email as a notice for the database update for this month. This update is designed by our IT engineers to provide higher security to our customers online accounts, prevent unauthorized account access and other types of online fraud.

You are required to update your online profile by clicking on the following link:

[Click here to access your online profile](#)

Please note that this a one-time task that will take only 3-5 minutes of your precious time. However, failure in updating your profile will result in limiting your account access. We appologize for any inconvenience.

*Thank you,
Jeremy M. Scott,
IT Assistant,
Western Union.*

Phishing

Or like this:

PayPal

Because it has expired, your credit card has been removed from your PayPal account.

If this was the only credit card on your PayPal account, you will need to add a new card to continue sending instant PayPal payments.

To add a new debit or credit card, log in to your PayPal account at www.paypal.co.uk, go to your Profile, and click **My money**.

Yours sincerely,
PayPal Direct

PROTECT YOUR PASSWORD

NEVER give your password to anyone, including PayPal employees. Protect yourself against fraudulent websites by opening a new web browser (e.g. Internet Explorer or Firefox) and typing in the PayPal URL every time you log in to your account.

Phishing

They invite you to click on the web-links

[Click here to access your online profile](#)

To initiate the confirmation process, [Click Here](#)

To add a new debit or credit card, log in to your PayPal account at www.paypal.co.uk, go to your Profile, and click [My money](#).

Never click on these links!

If you did click on the **paypal** link –
you'd arrive here:

Phishing



But you thought you were here

Phishing

The image is a screenshot of a web browser displaying the PayPal login page. The browser's address bar shows the URL: https://www.paypal.com/uk/cgi-bin/webscr?cmd=_login-run&dispatch=5885d80a13c0db1f8e263663d3faee8d4026841ac68a446f69dad17fb2afeca3. The browser tabs include 'Confirm Information. - Spam - Ya...', 'Login - PayPal', and another 'Login - PayPal'. The PayPal logo is prominently displayed at the top. Below it, there are navigation links: 'Sign Up', 'Log In', and a search bar. A horizontal menu bar contains links: 'Home', 'Personal', 'Business', 'Safety Advice', 'Where Can I Shop?', and 'Help'. Below this, a secondary menu lists: 'Homepage', 'Why PayPal?', 'Using PayPal', 'Managing Your Account', and 'Send Money'. On the left side, there is a 'Account login' section with fields for 'Email address' and 'PayPal password', a 'Go to' dropdown menu set to 'My account', and a 'Log In' button. Below the login fields are links for 'Problem with login?' and 'New to PayPal? Sign up'. On the right side, there is a large promotional banner for 'GET EXCLUSIVE DISCOUNTS FROM LEADING RETAILERS WHEN YOU SHOP WITH PAYPAL' with the URL 'Shop now at www.paypal-shopping.co.uk'. The banner features a couple looking at a laptop and logos for various retailers like ASOS, TK-MAXX, and Dorothy Perkins. At the bottom of the page, there is a footer with links: 'About', 'Account Types', 'Fees', 'Privacy', 'Safety Advice', 'Contact Us', 'Legal Agreements', and 'Developers'. A 'VeriSign Identity Protection' logo is also visible in the bottom right corner. A yellow callout box with a red border and black text is overlaid on the left side of the page, stating: 'This is the genuine web site'.

This is the genuine web site

If you click on the **Western Union** link, you are taken here

Phishing

secure5472online6687.blinxwebdesign.com/westernunion/?mfa=auth

tion Process - Spam - 'Yahoo! M... x Western Union Money Transfers | Send ... x +

WESTERN UNION | United Kingdom
moving money for better

Home | About Us | Investor Relations | Contact Us | Help
United Kingdom
Sign In Register | Money Transfer Find a Location Transfer Status

Sign In or Register

* indicates required field

Sign In to Your Account

Email Address: *

Password: *

[Sign In](#)


[Forgot your password?](#)

Don't Have an Account Yet?

Register with Western Union to transfer money: **Conveniently, Securely, and Reliably.**

[Register Now](#)

How Money Transfer Works



Complete Online Transaction
Sign in or register. Enter the details of your money transfer. Pay with your Visa® or MasterCard® credit card.

Call to Confirm Transaction
For your security, we may need to speak with you to confirm your transaction.

Receive Money
Receive money at any participating Agent location worldwide.

Protect Yourself from Fraud

Don't send money to someone you don't know. Find out how to help safeguard your transactions and your personal information to avoid online fraud.

[Learn more](#)

This is a web forgery

Home | Find a Location | Tracking | Careers | Fraud | Copyright | Privacy Policy | Terms & Conditions | Contact Us | Site Map

But you thought you were here

Phishing

Western Union Holdings Inc. (US) https://www.westernunion.co.uk/WUCOMWEB/osMTOptionsAction.do;jsessionid=24Y-AdUsLtUdGLngtYK8Kt?method=load&countryCode=GB&lar

Yahoo! Western Union Money Transfers | Send ...

WESTERN UNION | United Kingdom
moving money for better

Home | About Us | Investor Relations | Contact Us | Help
United Kingdom

Sign In Register | Money Transfer Find a Location Transfer Status

Sign In or Register

* indicates required field

Sign In to Your Account

Email Address: *

Password: *

[Sign In](#)

[Forgot your password?](#)

Don't Have an Account Yet?

Register with Western Union to transfer money: **Conveniently, Securely, and Reliably.**

[Register Now](#)

How Money Transfer Works

Complete Online Transaction

Sign in or register. Enter the details of your money transfer. Pay with your Visa® or MasterCard® credit card.

Call to Confirm Transaction

For your security, we may need to speak with you to confirm your transaction.

Receive Money

Receive money at any participating Agent location worldwide.

Protect Yourself from Fraud

Don't send money to someone you don't know. Find out how to help safeguard your transactions and your personal information to avoid online fraud.

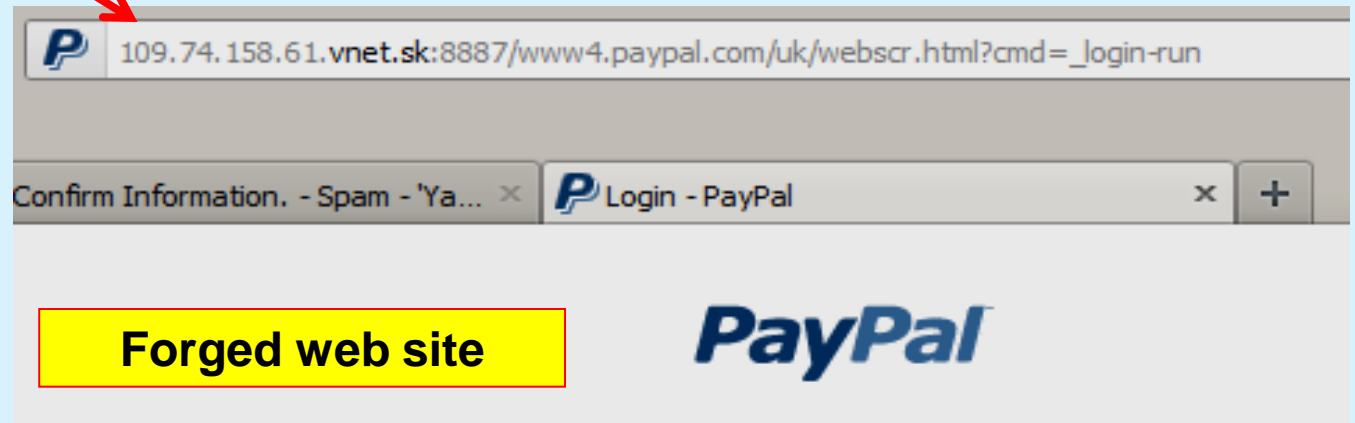
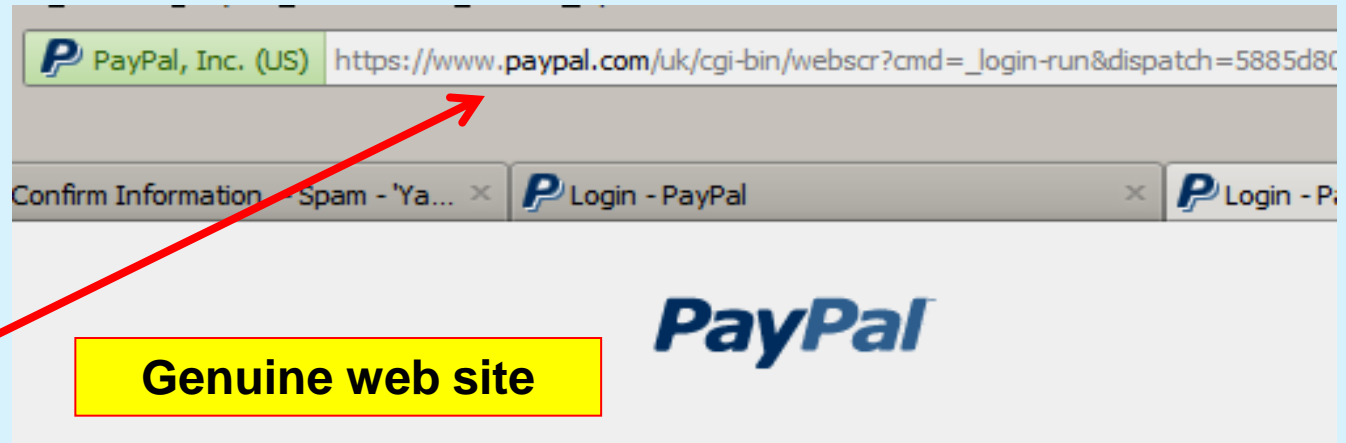
[Learn more](#)

Home | Find a Location | Tracking | Careers | Fraud | Copyright | Privacy Policy | Terms & Conditions | Contact Us | Site Map

This is the genuine web site

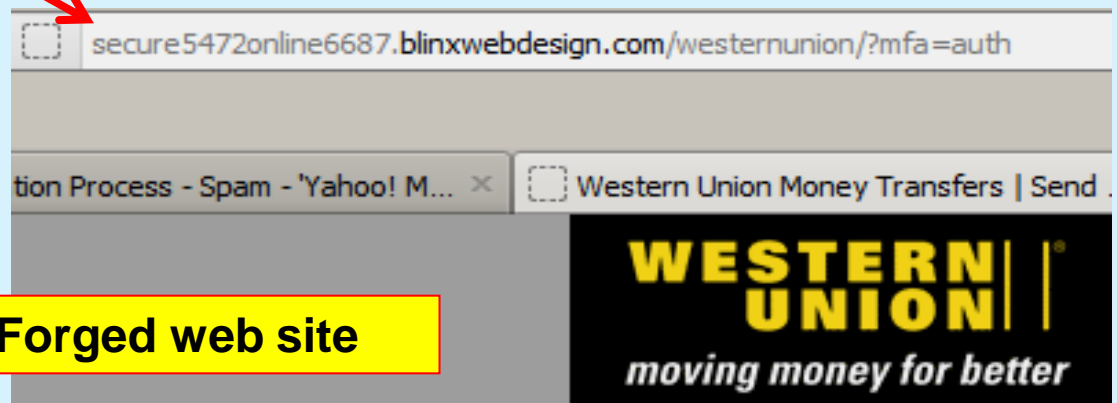
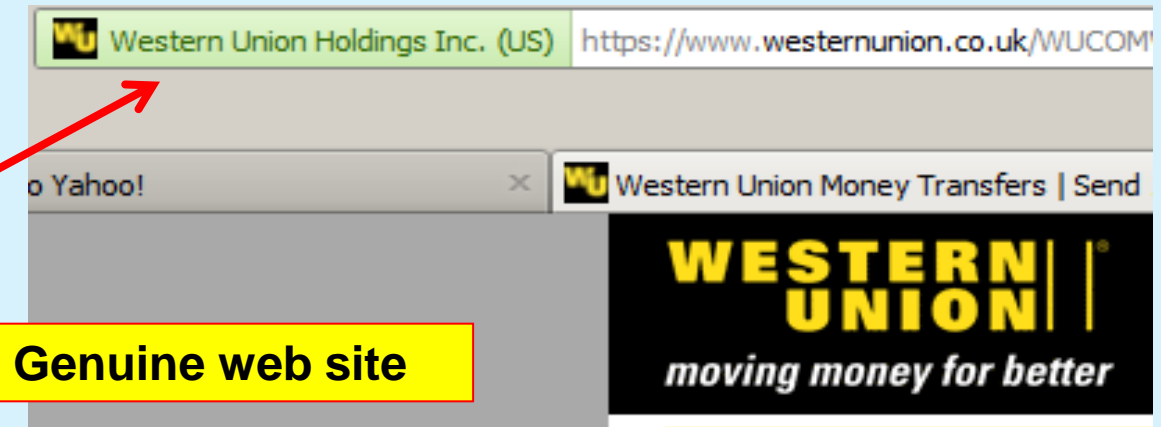
Phishing

Look at the **URL**.
The real website
address



Phishing

Again – look at the URL. The real website address



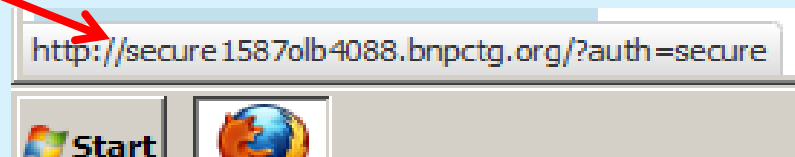
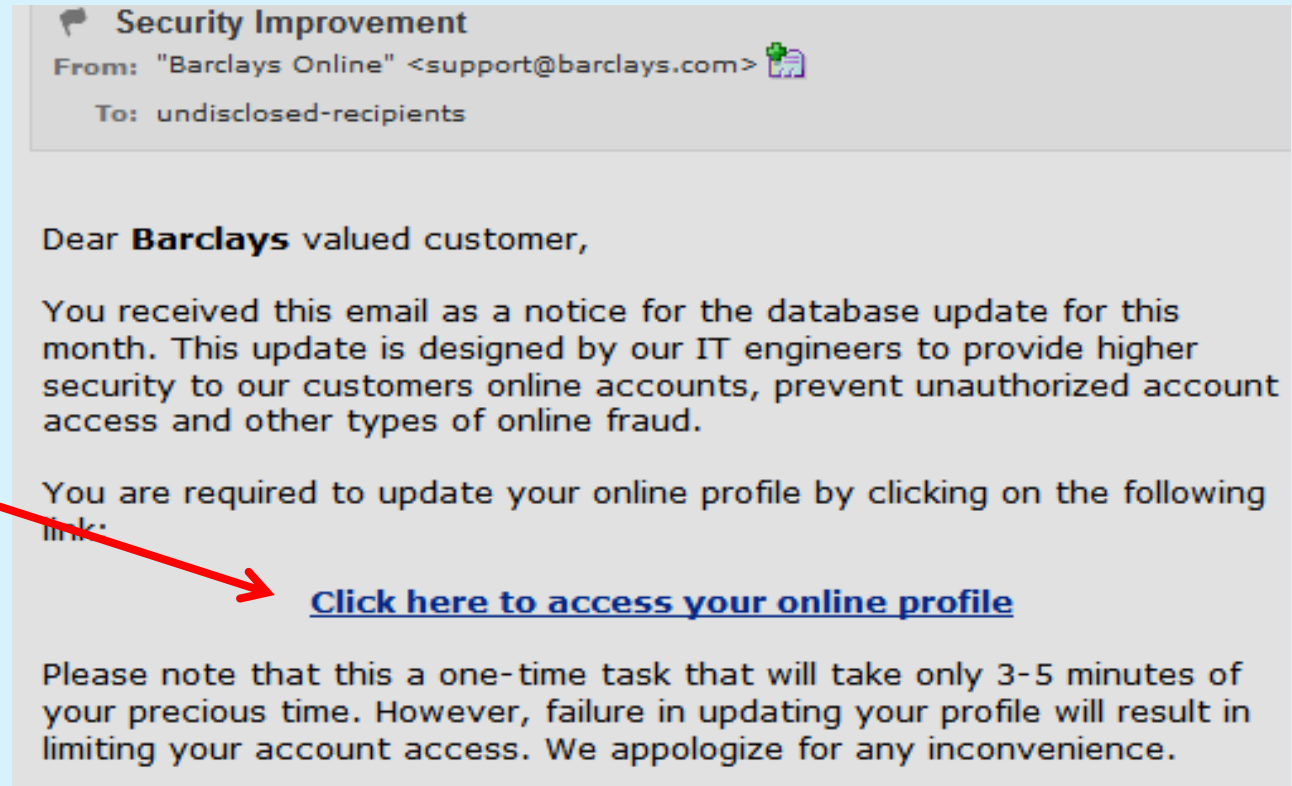
Phishing

But **before** you click...

Place your mouse over the link... But **don't** click

Look at the bottom of the browser

This is the web address you will be taken to



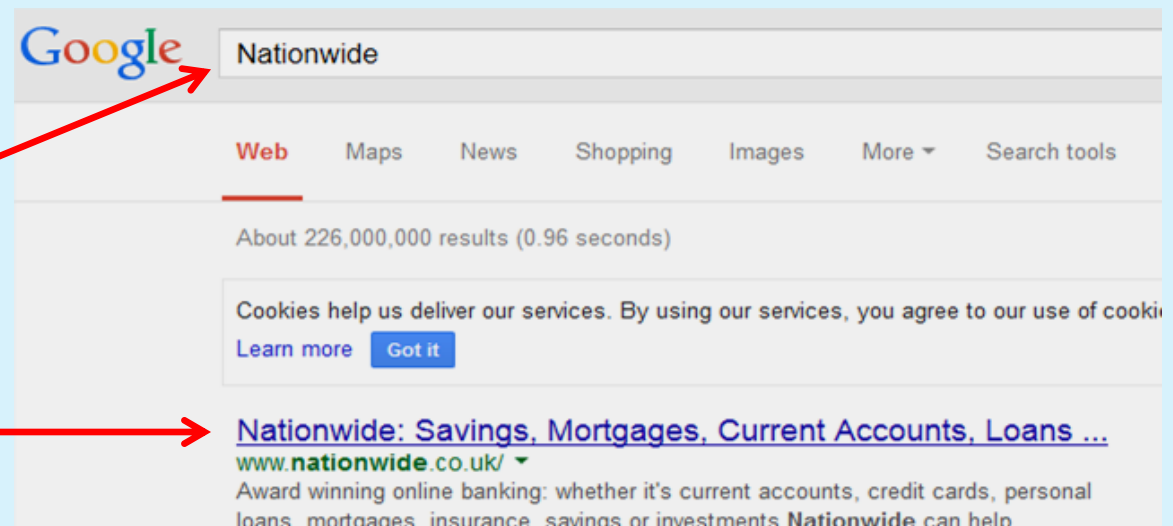
Obviously not Barclays Online

It is safest to type in the web address yourself



Or carry out
your own
web-search...

and follow the
link

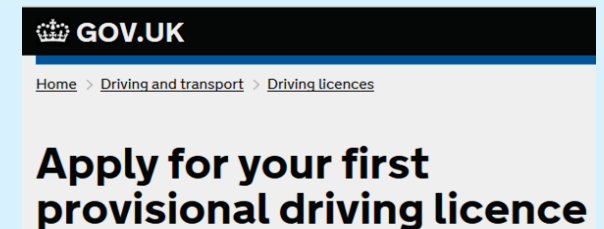
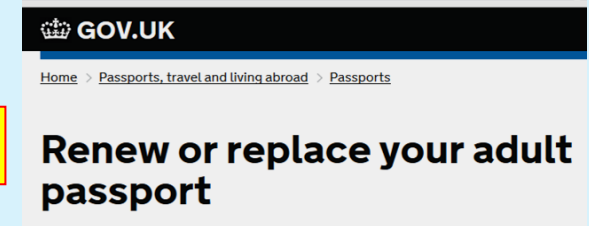
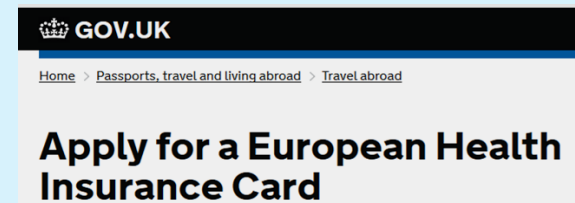
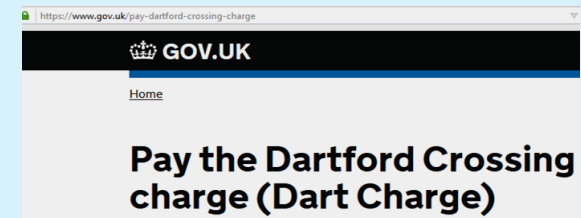


'Pretend' Websites via Google



Web sites
you don't
need to visit

Use .gov.uk



If you buy pharmaceuticals online, make sure you use a

Registered Pharmacy

They will have a **Green Cross** and their registration number



Check their validation on:

pharmacyregulation.org

Using Money Online

When you want to buy something on-line or enter any personal details, make sure the website address starts with **httpS**

<https://www.gov.uk/contact-the-dvla>

<https://www.amazon.co.uk>

<https://www.paypal.com/uk>

<https://www.nationwide.co.uk>

<https://www.hsbc.co.uk>

<https://www.surreycc.gov.uk>



<https://www.currys.co.uk>

<https://www.diy.com>

This means it is a **secure site** – and no-one can intercept your details

Using Money Online

But, although https means your data cannot be intercepted – it doesn't mean it is a **trustworthy** site.

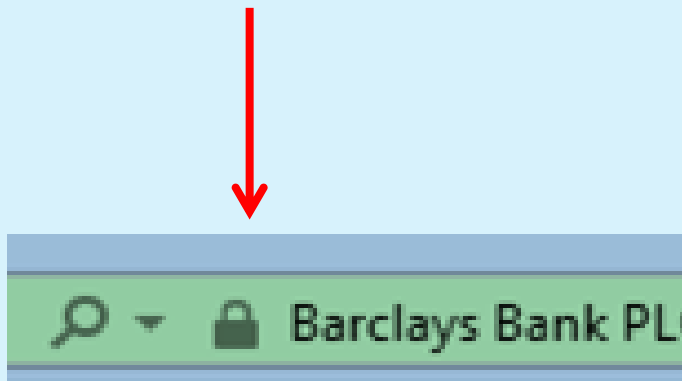


https://payments.ebay.co.uk/w

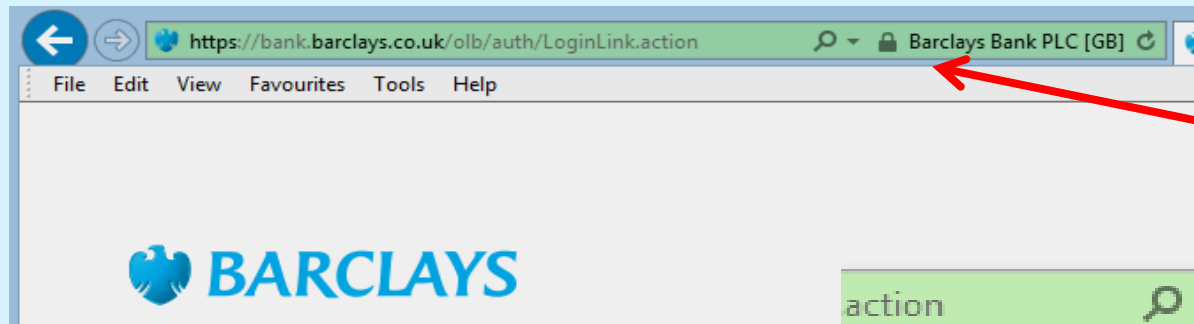


https://www.westernunion.co.uk/W

Even the small green padlock is not a guarantee that the site is trustworthy



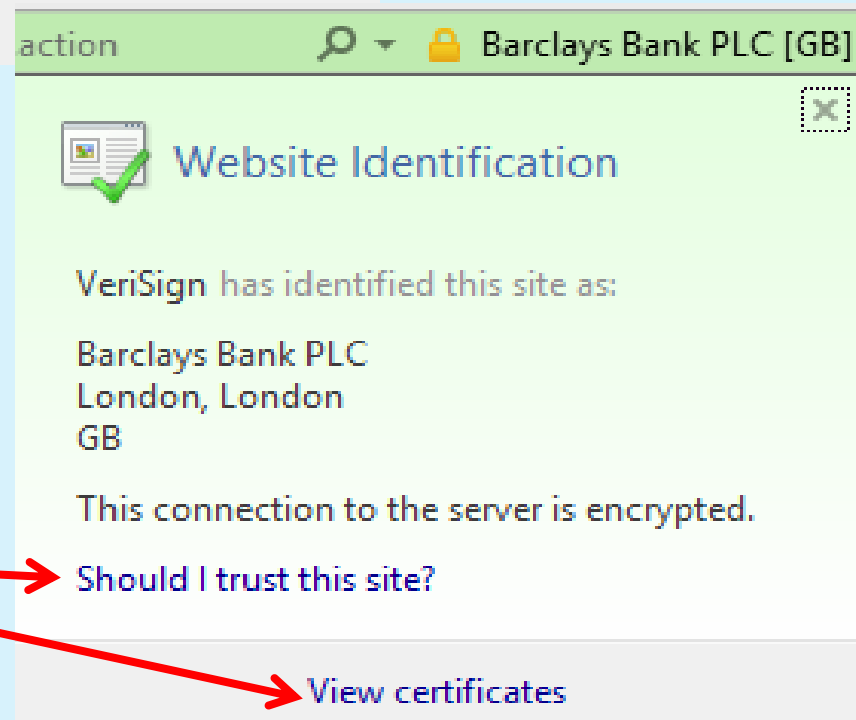
Using Money Online



But click on the padlock....

You will see more information – check the details

And follow the links for more detailed information



It should give you confidence that it is a genuine site

Using Money Online

Use a credit card instead of a debit card if you can. Seller won't know your bank details and the card company will have a method of dispute resolution

For an extra layer of security:

Sign up to an online payment platform:

PayPal / Apple Pay / Google Pay

Use it to pay the supplier, if it's an option

A screenshot of the PayPal sign-up form. At the top, it says 'Sign up' with a small PayPal logo. Below this are several input fields: 'Country or region' with a dropdown menu showing 'United Kingdom', 'Your email address', 'Create your PayPal password', and 'Add and confirm your phone number'. The phone number section has a 'Code' dropdown showing '+44' and a 'Phone number' field. At the bottom is a blue 'Next' button.

It puts a trustworthy agent between you and the supplier

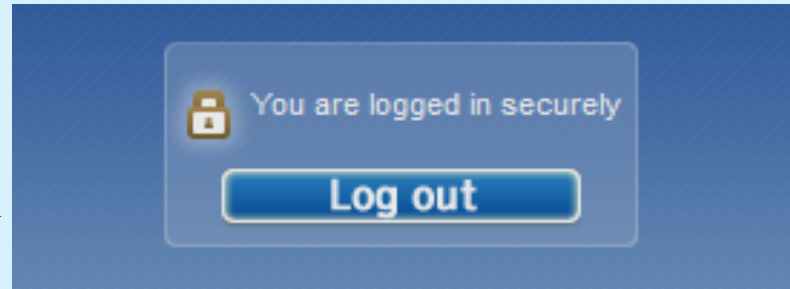
They all have a dispute resolution centre

Logging Out

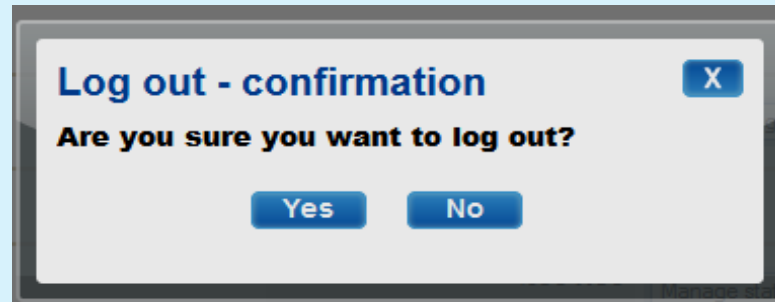
If you have logged into a secure website

Always ensure you log out correctly

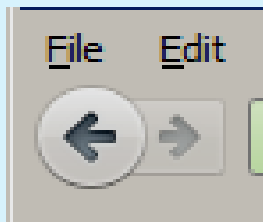
Left click on the 'Log out' button →



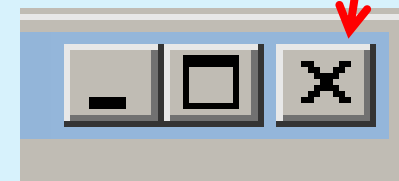
You may have to confirm your action



Do **not** use the back button



Do **not** 'crash' the browser by clicking on the 'X'

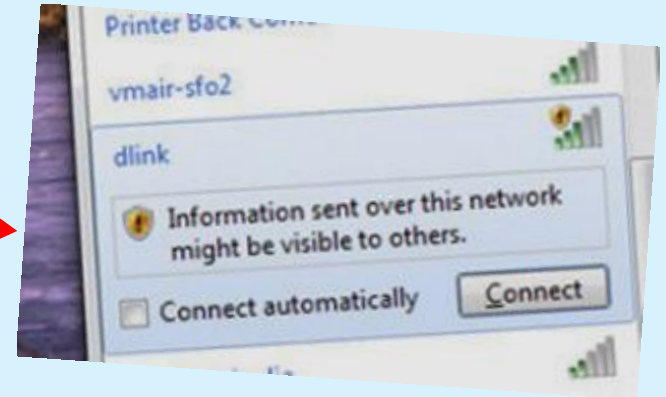


Public Wifi



Public internet access is inherently unsafe

You and the (potential) hacker are
inside the same firewall



If you use public WiFi, **never** do
anything confidential or use a
debit or credit card



Safer Internet Browsing

We've all heard of service providers being hacked.
Maybe your data was stolen...

TalkTalk given record fine over data breach that led to data theft of nearly 157,000 customers

The personal data of 156,959 customers including names, addresses, dates of birth, phone numbers were stolen

eBay hack 'one of the biggest data breaches in history'

Equifax Data: one of the worst security breaches in history



British Airways has settled a legal claim by some of the 420,000 people affected by a major 2018 data breach.

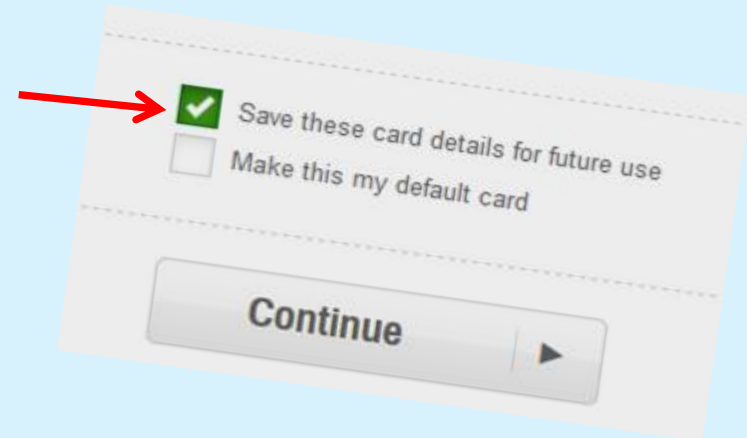
The breach affected both customers and BA staff and included names, addresses, and payment-card details.

The Information Commissioner's Office handed BA its largest fine to date, of £20m, over the "unacceptable" failure to protect customers.

Facebook Security Breach Exposes Accounts of 50 Million Users

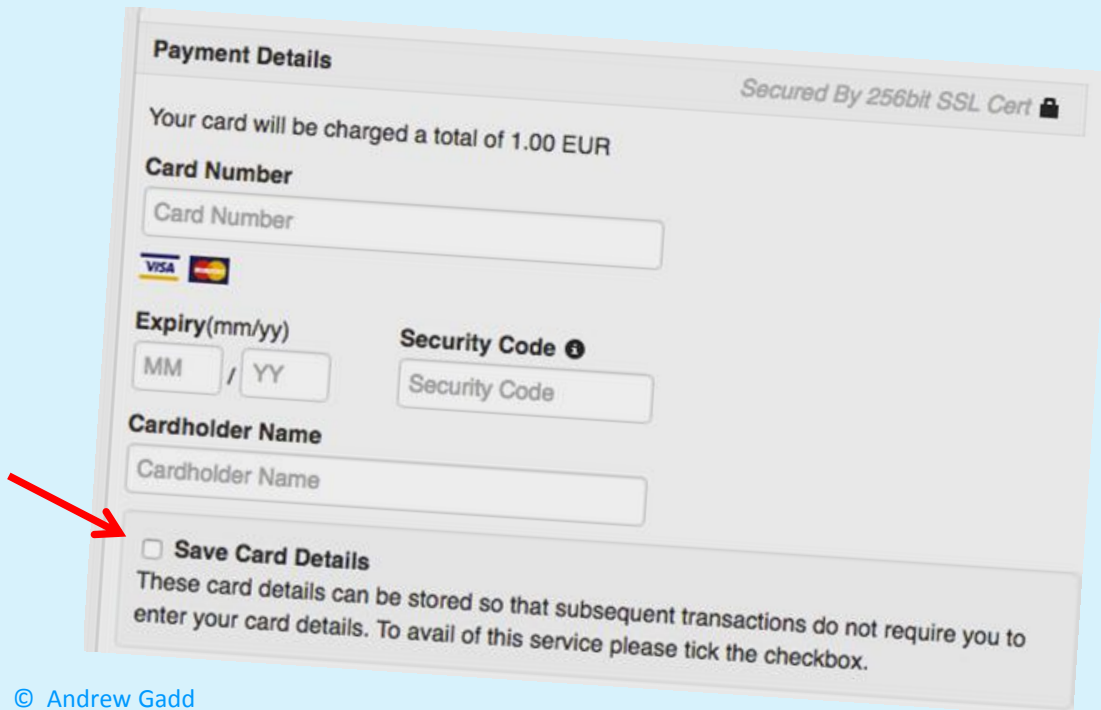
Safer Internet Browsing

It is not quite as convenient, if you **don't** allow the provider to store your card details, you'll be a little less exposed. Make sure the 'Save' boxes are not ticked. GDPR rules say you have to 'opt-in' but always check



☒ Save these card details for future use
☐ Make this my default card

Continue



Payment Details

Secured By 256bit SSL Cert

Your card will be charged a total of 1.00 EUR

Card Number

Card Number

VISA

Expiry(mm/yy)

MM / YY

Security Code ⓘ

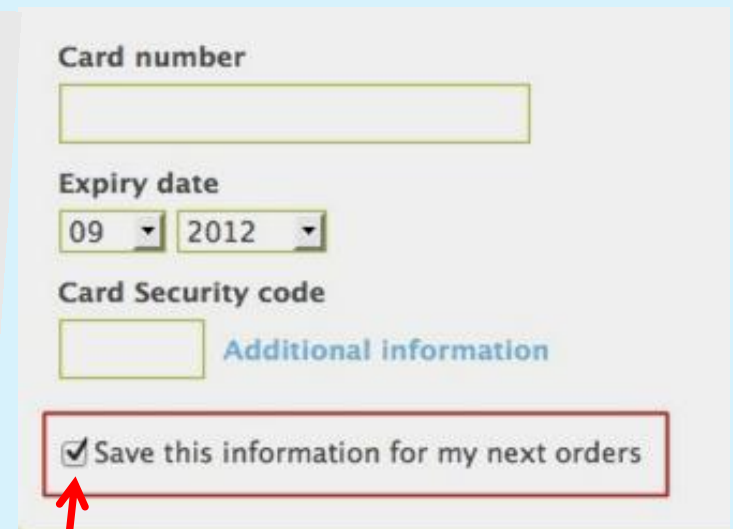
Security Code

Cardholder Name

Cardholder Name

☐ Save Card Details

These card details can be stored so that subsequent transactions do not require you to enter your card details. To avail of this service please tick the checkbox.



Card number

Expiry date

09 2012

Card Security code

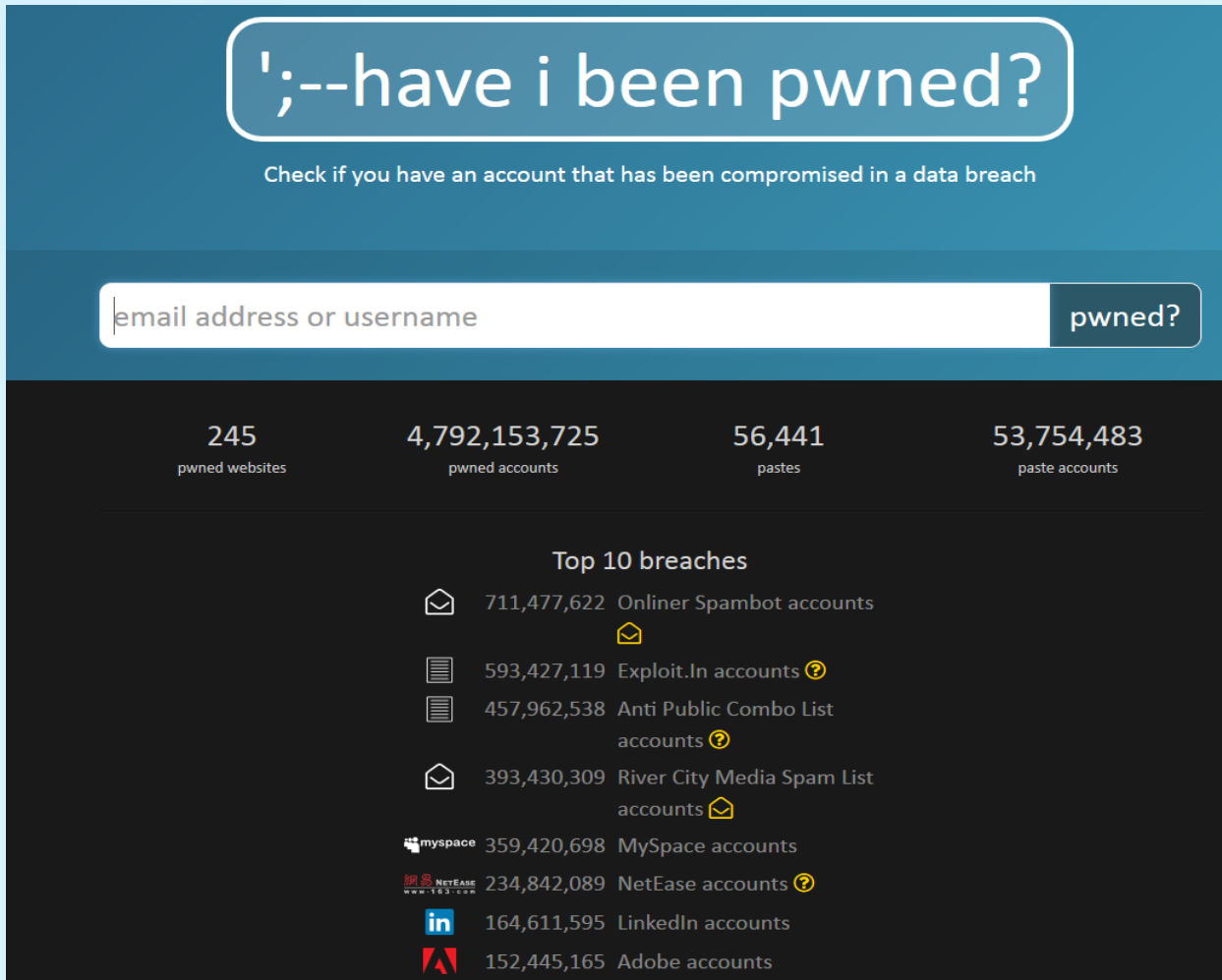
Additional information

☒ Save this information for my next orders

Safer Internet Browsing

Visit
haveibeenpwned.com

Enter your email address into the box and click on 'pwned?'

A screenshot of the haveibeenpwned.com website. The header is blue with the text '';--have i been pwned?' in a white rounded box. Below it, a subtitle reads 'Check if you have an account that has been compromised in a data breach'. The main section has a dark background with a search bar containing the placeholder 'email address or username' and a 'pwned?' button. Below the search bar, statistics are shown: 245 pwned websites, 4,792,153,725 pwned accounts, 56,441 pastes, and 53,754,483 paste accounts. A section titled 'Top 10 breaches' lists various data breaches with their respective counts and icons.

Top 10 breaches	
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts ?
457,962,538	Anti Public Combo List accounts ?
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts ?
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts

Safer Internet Browsing

And hope you don't see this message!

If you do, you need to change your password!

Oh no — pwned!


Pwned on 3 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

[Notify me when I get pwned](#) [Donate](#)

[Facebook](#) [Twitter](#)


Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames



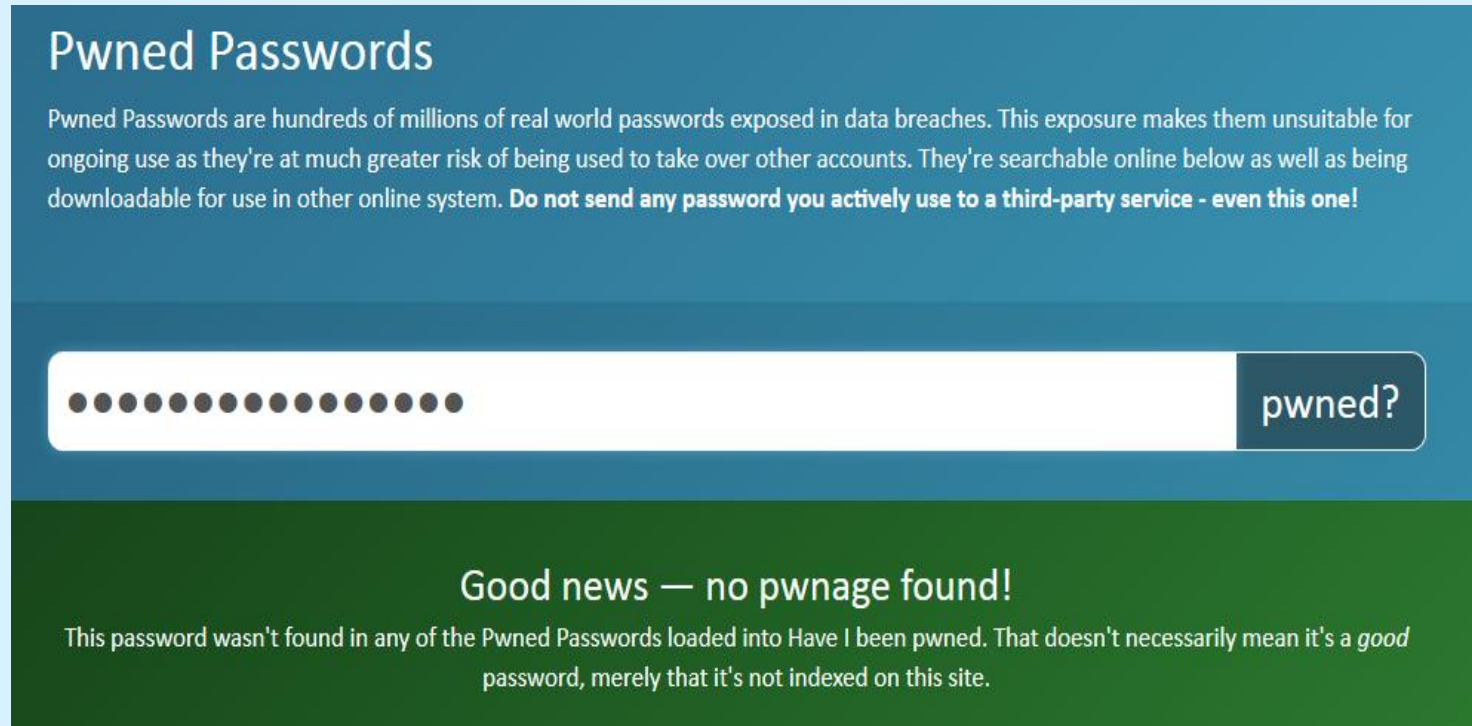
Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Safer Internet Browsing

haveibeenpwned.com

On the same site, you can see if any password you use has been found on a pwned site



The screenshot shows the 'Pwned Passwords' section of the Have I Been Pwned website. It features a blue header with the title 'Pwned Passwords' and a paragraph explaining that pwned passwords are exposed in data breaches and are unsuitable for ongoing use. Below this is a search interface with a long white input field containing 15 black dots, a dark blue button labeled 'pwned?', and a green footer area. The footer area contains the text 'Good news — no pwnage found!' and a disclaimer stating that the password was not found in the database, but this does not necessarily mean it is a good password.

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. **Do not send any password you actively use to a third-party service - even this one!**

..... pwned?


Good news — no pwnage found!

This password wasn't found in any of the Pwned Passwords loaded into Have I been pwned. That doesn't necessarily mean it's a *good* password, merely that it's not indexed on this site.

This does not tell you if a password is any good. Just if it's been found in a data breach.

Email Scams

This sort of email is 20+ years old, but the scammers still send them out

From: "Mrs.Anizar Hussan" <info@anizar.com> 

To: undisclosed-recipients

My Beloved I am Mrs. Anizar Hussan a citizen of Oman but currently residing in the United Kingdom.I have a business proposal for you worth US\$40.8Million.Please if you are interested contact me through aniza.hussan0108@hotmail.com so that we can discuss more about the business.

Remain blessed,
Mrs. Anizar Hussan

It is obviously a scam. (\$40million!) So, why do they keep sending them out?

Do **NOT** respond.

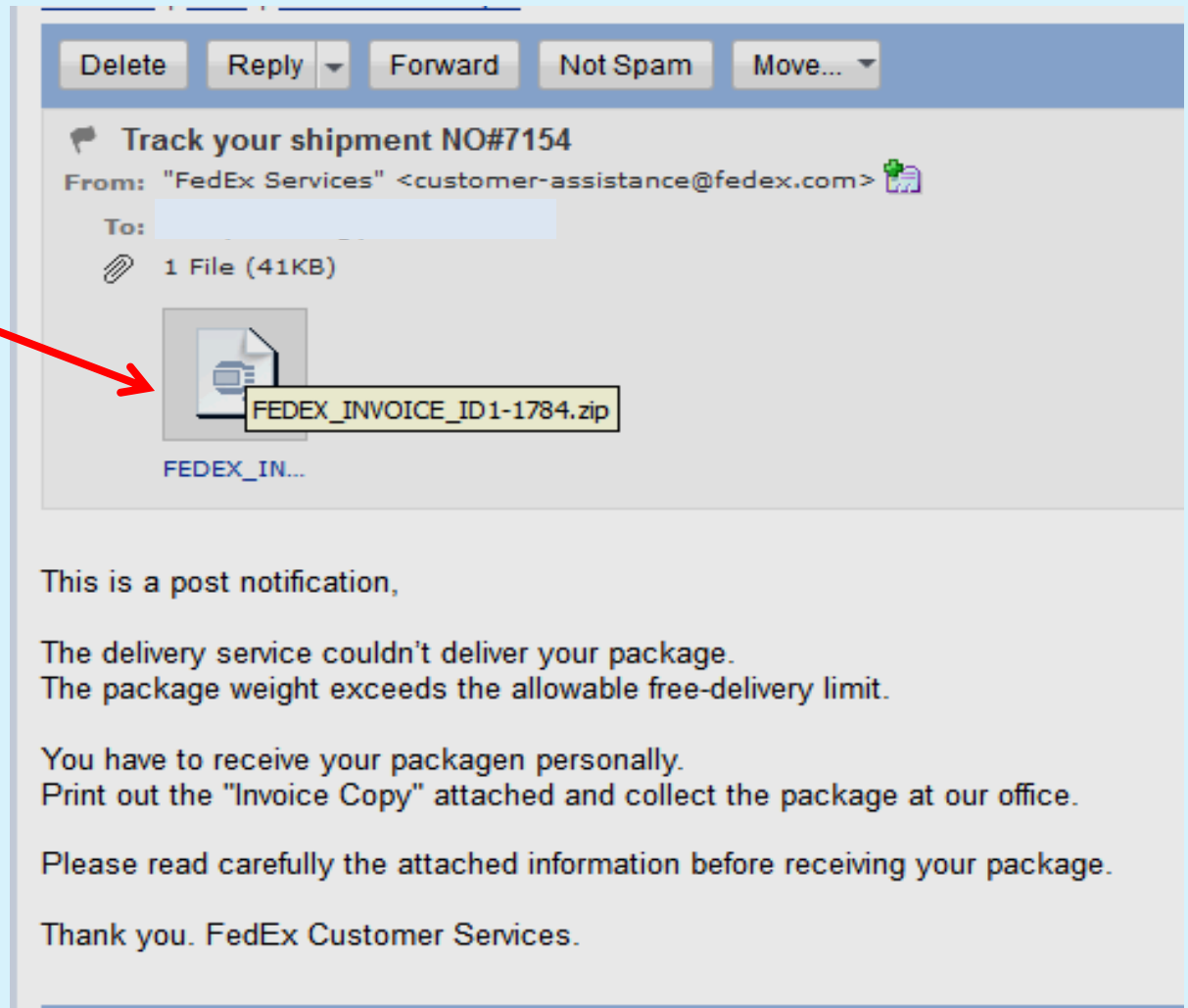
If you reply, you confirm your email address – and it will be sold to others

It is estimated that 72% of all email is Spam

Email Scams

**NEVER open
strange
attachments**

**It will undoubtedly
infect your device
with a virus**



Email Scams

Some Spam emails are
almost believable

It has the HMRC logo

It is offering a tax refund
of (only) £364.77

BUT:

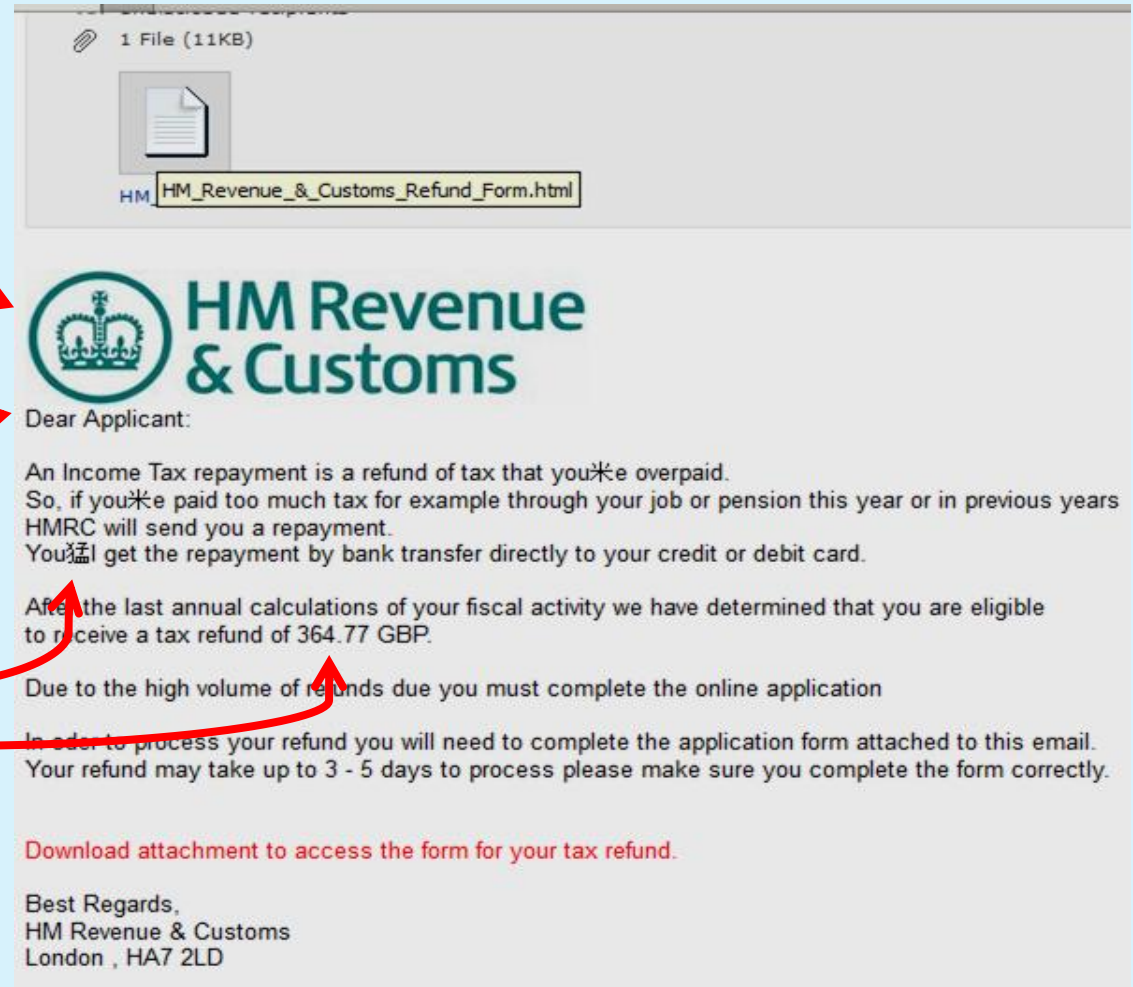
It's not addressed to you

It uses the wrong characters

The sender did not have a '£' on
their keyboard – which makes it
very suspicious

This is a spam email

**Downloading the
attachment would infect
your device**



Email Scams

The 'scammers' are getting better all the time

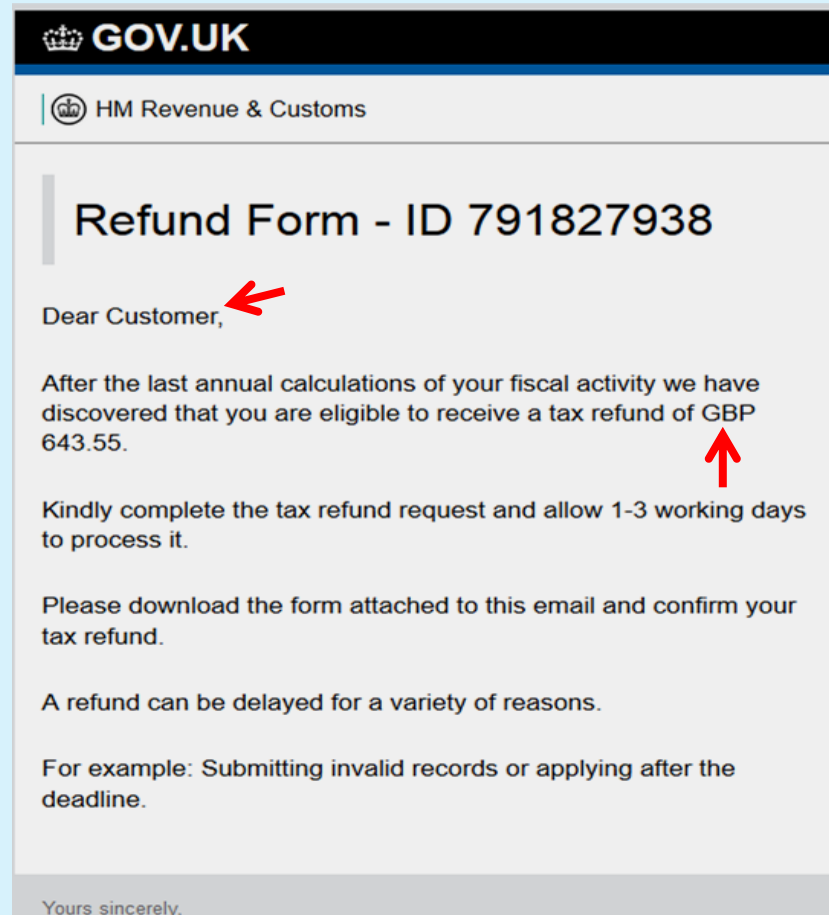
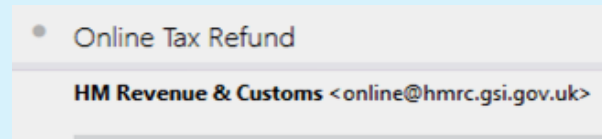
It has a genuine looking email address

Correct logo

No spelling or grammar mistakes

A believable £643.55

BUT: Not addressed to you & no '£' sign



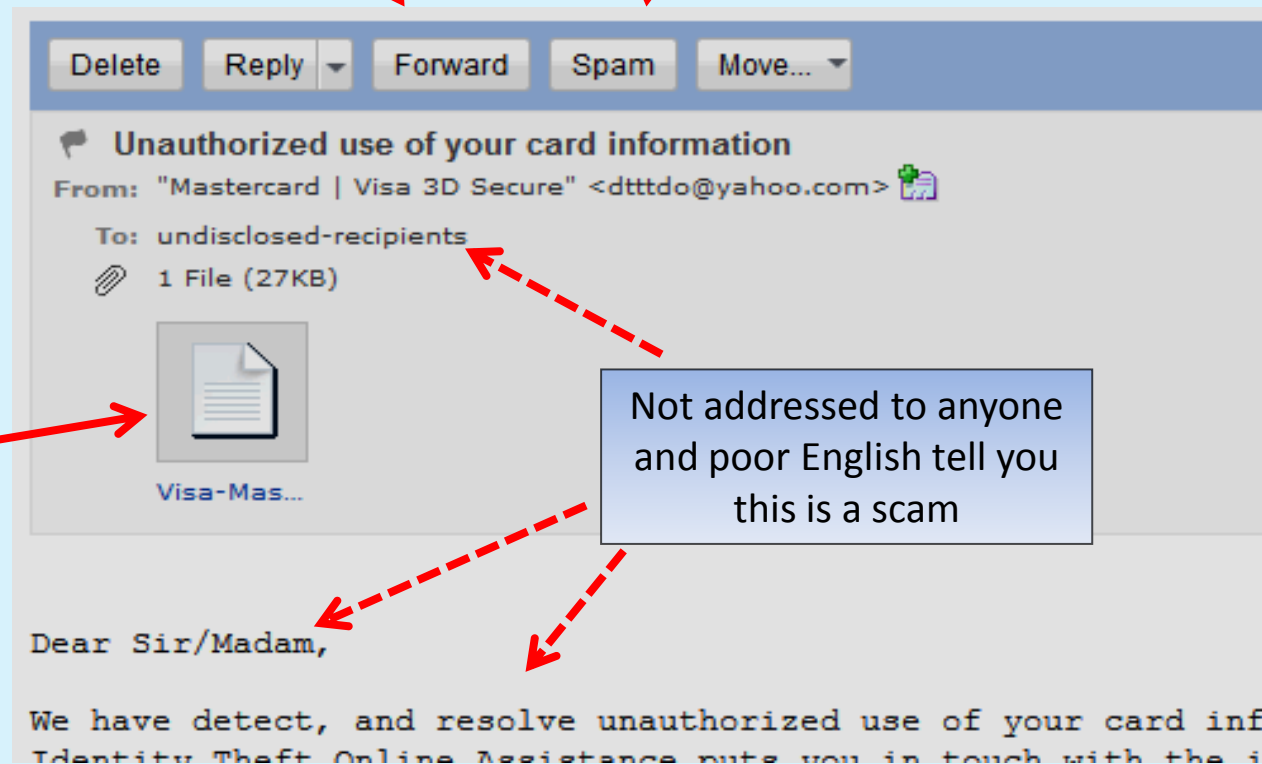
Email Scams

Forward this to report@phishing.gov.uk and the National Cyber Security Centre (ncsc.gov.uk) will try to get the sender shut down.

Then click on 'Spam'. This email will be sent to your Spam folder

All future emails from this address will be sent straight to the spam folder

Another VERY suspicious attachment. Don't click on it.



Email is Not Secure

Why does your bank never email your statement to you?

Because email is not secure

You might log-on to an https website, but the email will be forwarded on to many computers during it's journey

It *travels in plain text* over the network and will be *stored in plain text* on email servers

Think of your email as a postcard!

For a secure email, search for: Proton Mail, Startmail, Tutanota, Zohomail or Thexyz



<https://mail.google.com/>

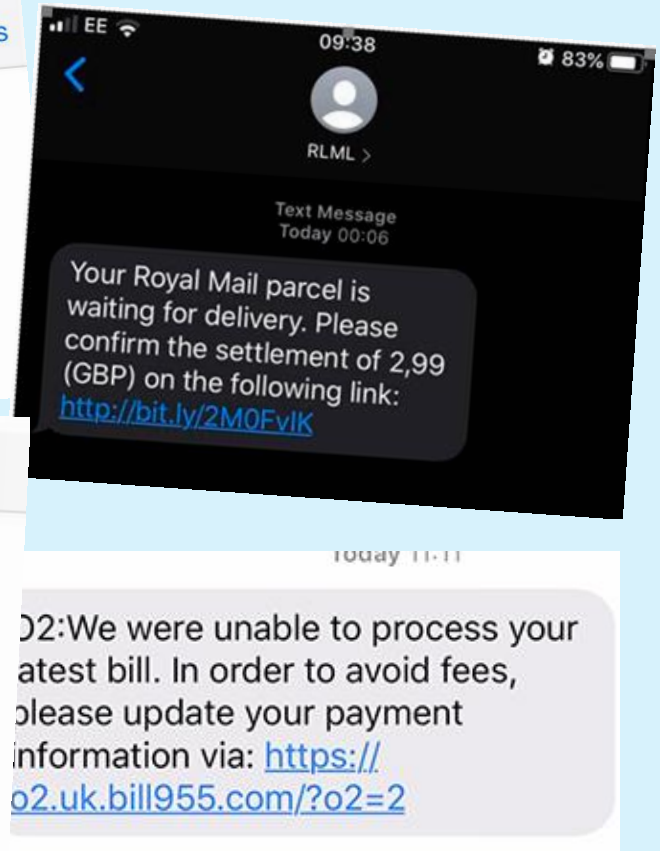
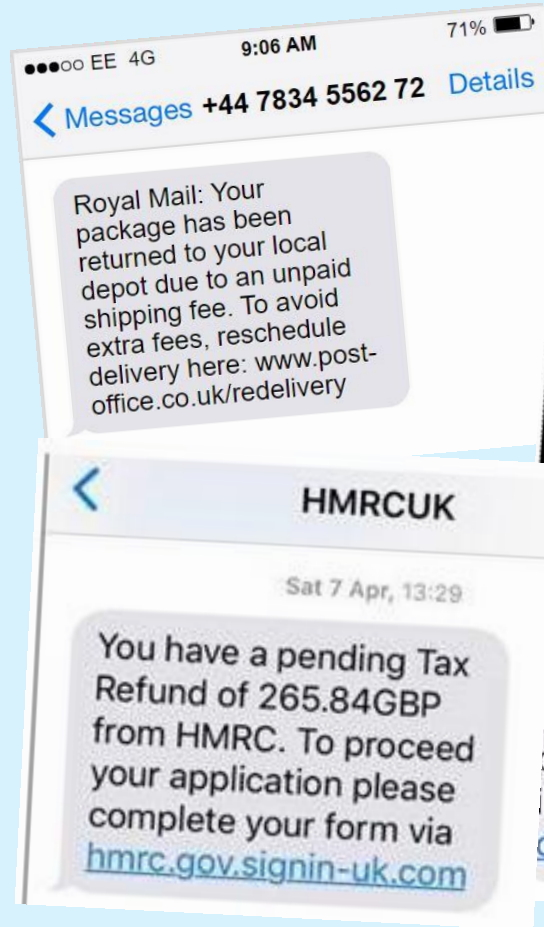
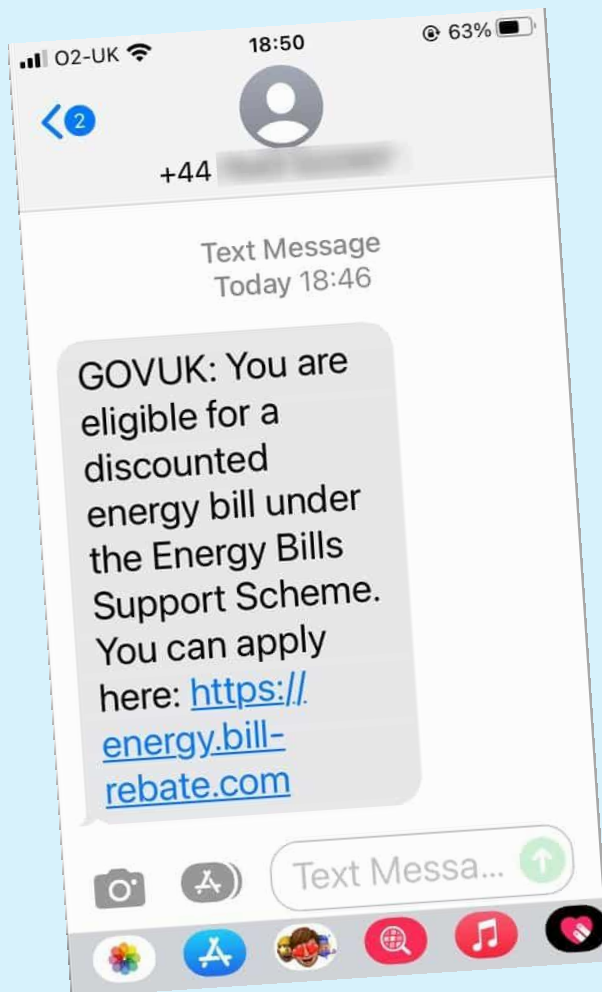
<https://mail.yahoo.com/>

Some are surprised to learn that Google and others scan your emails for keywords to show more personalised adverts



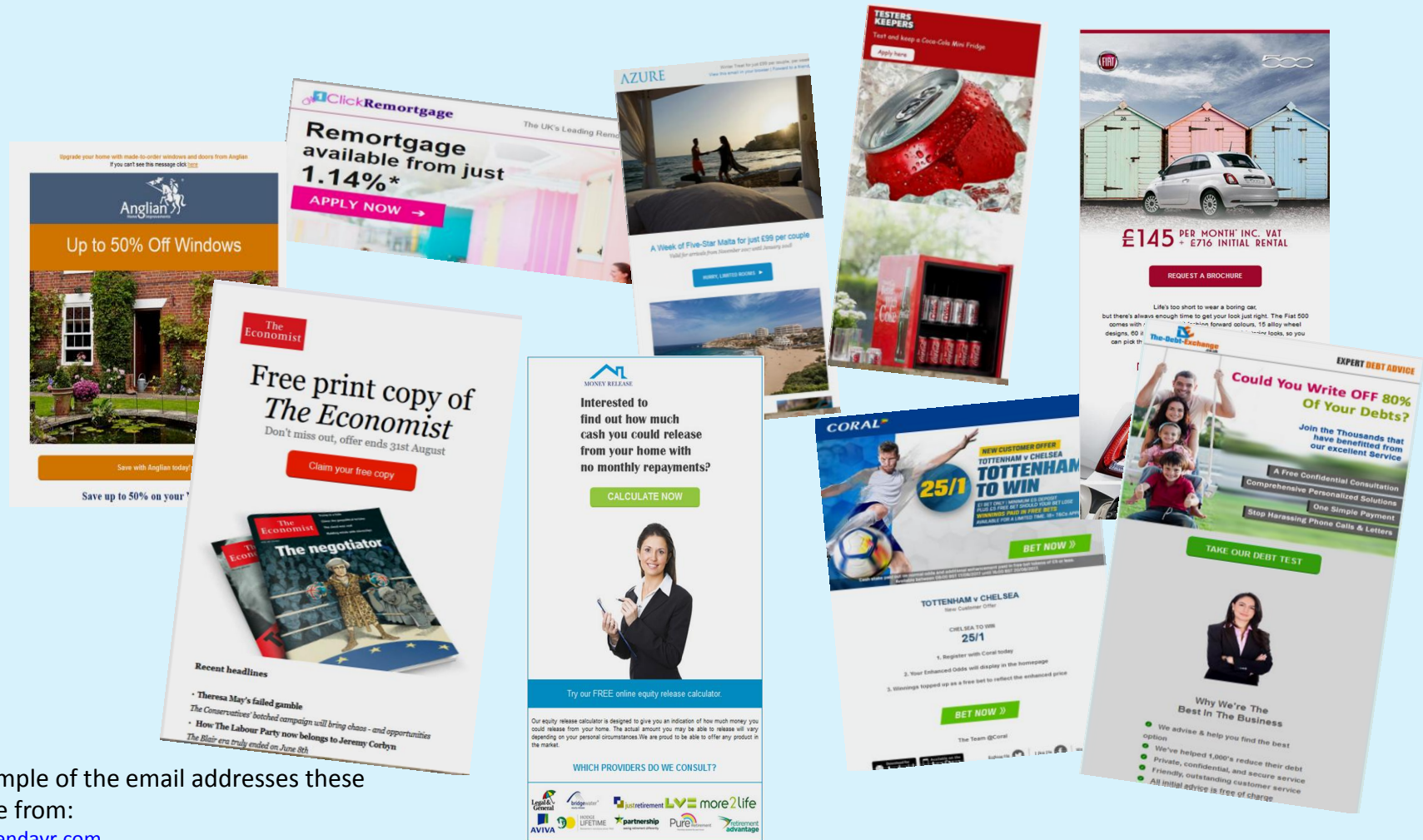
Text Scams

If you receive a phishing / scam text, NEVER respond. Forward them 7726 and the National Cyber Security Centre will get the sender shut down.



And they are getting better all the time.....

Email Scams



A sample of the email addresses these came from:

@calendavr.com
@getspora.com
@infor.cirnas.com
@skyNet.thayaalu.com
@infor.agencebe.com

Constantly evolving scams,
exploiting every opportunity

SCAM WARNING

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

**Coronavirus-related frauds
increase by 400% in March**

SEARCH

HEAD TOPICS UNITED KINGDOM



Ukraine war: Investigation finds hundreds of fake charity websites



Business / Finance

Council tax rebate: Warning issued over new scam pretending to offer 150

Scammers are cold-calling people asking for their bank details to receive the government's 150 energy rebate, councils have warned....



Security Software

An anti-virus program is essential

There are many to choose from

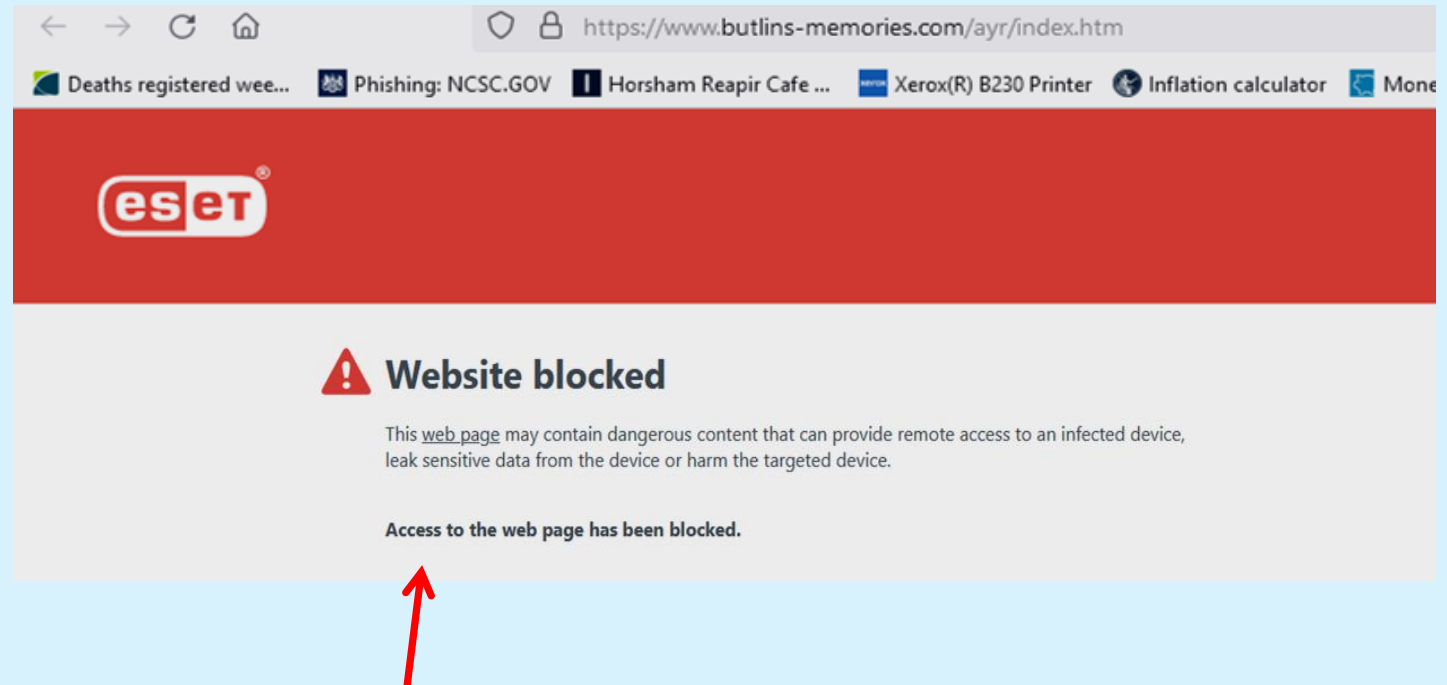
Some cost money...



Security Software

When a spam email asks you to visit a website OR
you download an unknown attachment

If you try to visit a
website that has
'dangerous
content'....



Hopefully your anti-virus program will stop it

Note the website is a very innocent sounding [butlins-memories.com](https://www.butlins-memories.com)

Security Software

Some are free for domestic use



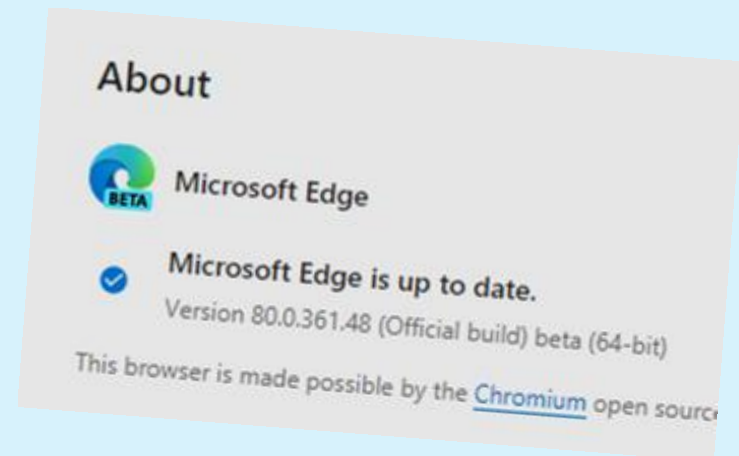
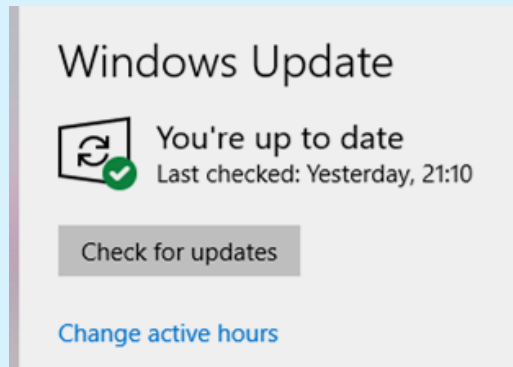
In my opinion, either of these free programs are probably adequate for domestic use.

But you will see various 'pop-ups' encouraging you to upgrade to a paid version

Software Updates

It is vital to keep your software up to date.

Most updates fix security flaws



Adobe Flash Player

Bundle up
Photoshop and Lightroom together
£8.57/month
[Buy now](#)

ADVERTISEMENT

Adobe Flash Player is the standard for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.

The table below contains the latest Flash Player version information. Adobe recommends that all Flash Player users upgrade to the most recent version of the player through the [Player Download Center](#) to take advantage of security updates.

Platform	Browser	Player version
Windows	Internet Explorer - ActiveX	17.0.0.134
	Internet Explorer (Windows RT) - ActiveX	17.0.0.134

Version Information
You have version 16.0.0.305 installed

Java Versions on Your Computer

Congratulations!
You have the recommended Java installed
Version 8 Update 40

No out-of-date versions of Java were found.

[Return to the Java.com home page](#)

Security for Mobiles

Beware of fake downloads...

Be careful of what you download even from the official app store

Strongly suggest you install some security software on your mobile

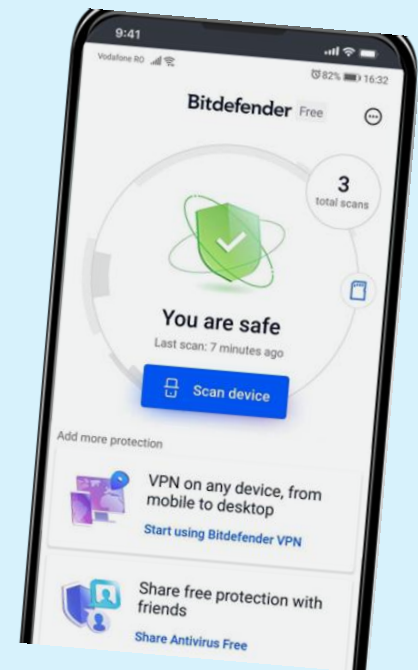


It might look like the genuine 'app'
**but many crooks create fake apps
that look like the real thing**



Ideally, go to the **vendors website**
and follow the link to the app store

© Andrew Gadd



Social Media Safety



Use extra precautions when using social media on mobile devices

Don't:

Tweet photos from inside your home

Mention your address on any social network

Announce when you're going on holiday

'Check-in' at airports or holiday destinations on social channels

Post your holiday pictures whilst on holiday

Post photos of new expensive items you've bought or received

Assume the safety settings of your social profiles are where you left them

According to the Surrey Police...



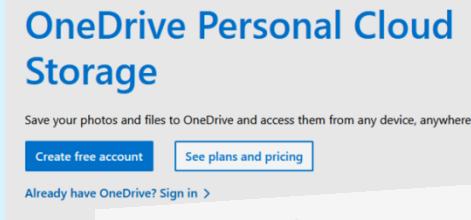
Backups

What would happen if your device died or was stolen?

What if your data was encrypted by a hacker?

It depends on your device...

Use online storage



Your stuff, anywhere

First name

Last name

Email

Password

☐ I agree to Dropbox terms.

Sign up

or Sign in

Use an external drive for a lot of data

Use a USB 'Flash Drive' for less data



SanDisk Extreme 1TB Portable SSD Hard Drive

★★★★★ (6)



SanDisk Ultra 100MB/s USB 3.0 Flash Drive - 128GB

★★★★★ (252)

A backup copy of your data might 'save the day'!

The Essential Guide to On-line Safety

The logo for 'welivesecurity' in a blue, lowercase, sans-serif font.The logo for 'Action Fraud' in red and black, with the text 'National Fraud & Cyber Crime Reporting Centre' and the phone number '0300 123 2040' below it.

For further study, the following websites are recommended:



actionfraud.police.uk

cyberaware.gov.uk

getsafeonline.org

thinkuknow.co.uk

thinkjessica.com

bbc.co.uk/webwise

welivesecurity.com

takefive-stopfraud.org.uk

ncsc.gov.uk

disney.co.uk/internet-safety



Get Safe Online
Free expert advice



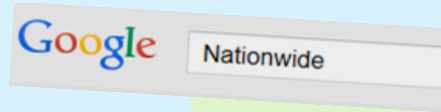
Internet Safety

Be secure when you explore

**Don't forget your bank or building society
will have their own security pages!**



The Essential Guide to Online Safety



I hope this presentation
has been useful

Any feedback (good or bad) is gratefully received at:

presentationfeedback2023@gmail.com

Thank you in advance!"

