Keeping safe online …

… tracking, scams and phishing exposed …

and how can we protect ourselves

About me … and Thought grazing

Until I retired (ten years ago) I was an IT Director with responsibility for strategy, and engagement with the staff and students at Cardiff University - we called it “enablement”.

I had responsibility for developing the university’s emerging use of social media.

I have developed a number of websites in the past twenty plus years and now run a website … **Thoughtgrazing** for third agers - https://thoughtgrazing.com

Anyone can visit the site. It has posts of general interest for “third agers” and their use of Information Technology (IT), including a transcript of this talk.

The plan - where is the talk heading?

Part 1: The threats - real and perceived

Questions and comments

Part 2: Should you be frightened

More questions and comments

Part 3: Measures to protect yourself

Questions, comments and discussion

Part 1: The threats - real and perceived

Here I aim to talk about some annoyances that don't really do any harm but are pervasive all the same and if we can avoid them our lives might be much more pleasurable!

Unfortunately often the perceived threat is more debilitating than the actual (or real) threat and prevents us making the most of some amazing technology, without which we couldn't in many instances have got through the pandemic.

- *What is the difference between Privacy and Security? Are they connected?*
- *Is there a trade-off with Privacy you have to accept? Can absolute Privacy ever be achieved?*
- *Is there a level of reduced Security which is acceptable?*
- *What are cookies? What is GDPR and giving Consent for trackers and profilers? Do you have to accept adverts?*

Where do you place yourself on this scale ...

Terrified -> Apprehensive -> Sensibly Aware -> Relaxed -> Unconcerned

I aim to get you to Sensibly Aware today on the road towards Relaxed and Unconcerned as your understanding develops.

Security and privacy

You should never compromise on **security** - that’s an absolute thing; if you do, you’re leaving the door open to scams, fraud and unhappiness. The weakest point in IT Security is YOU. You need to be able to protect yourself against yourself.

Privacy is giving-up information about yourself that you may, or may not, want to share with an organisation, corporation or company. Generally, this does not lead to reduced levels of security, but you should be open to reviewing the information you knowingly, and more often unknowingly, give-up to these bodies.

For instance … Opening a browser you may be asked to accept … Cookies

… and then challenged to remove … Ad-blockers (if you’ve installed them) [*more about these later*]

It’s your decision; it’s down to GDPR rules and putting the consumer back in charge and enhancing Privacy so that websites can’t track what we do unless we give them explicit permission to do so.

Privacy

Let’s start with **Browsers** - you don’t have to use Google Chrome, or worse still the Google app on your phone. Plenty of alternatives that are safe, secure and don’t track you across the internet, eg Brave, Firefox, Safari, Edge, Opera.

Then **Search Engines** - you don’t have to use Google, Bing or Yahoo. Why not try DuckDuckGo which doesn’t keep a record of your search history so can’t pass it on to third-parties.

Then **Ad-blockers** - look at Extensions to your browser, or add an app to your phone to prevent unwanted adverts popping up on your screen, or alternatively or in addition, think of changing your browser to Reader View.

And then there are **Cookies** (also Tracking Pixels) which keep a track of what you’re doing, and which the GDPR was introduced to control unfettered data gathering.

Let’s do a demo …

Firefox - Protect your life online with privacy-first products

Browsers The Best Search Engines of 2021

DuckDuckGo — Privacy, simplified.

Adblock Plus | The world's #1 free ad blocker

What Are Cookies?

How to know if tracking pixels watch your emails

Questions?

Don’t even get me started on Facebook, Instagram, WhatsApp and twitter!

… so we’ll put aside Privacy, recognising you may have to relinquish some to get free services on the internet, and turn to Security, a different kettle of fish!

Part 2: Should you be frightened?

Here we're going to look at how safe it is to use the Internet for banking, shopping, other activities.

What is safer (more secure) - an app on a mobile phones or online access through a web browser?

What are the threats, the potential vulnerabilities; the identification of threats - eg scams and phishing attacks

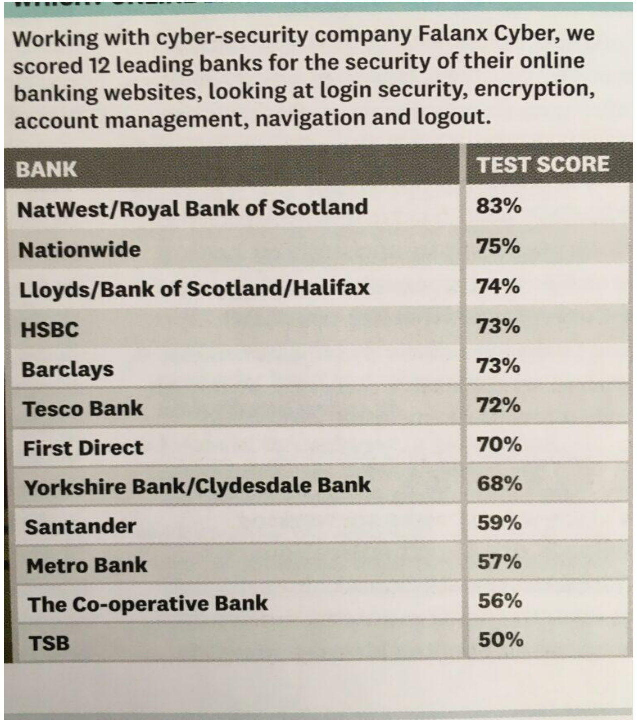
It's not just emails and web pages - it's texts and phone calls too

Should you be ...

Frightened - NO … Cautious - YES!

… and still to come in Part 3: Measures to protect yourself - How do you mitigate the risk(s)

Security of online banking (and shopping)



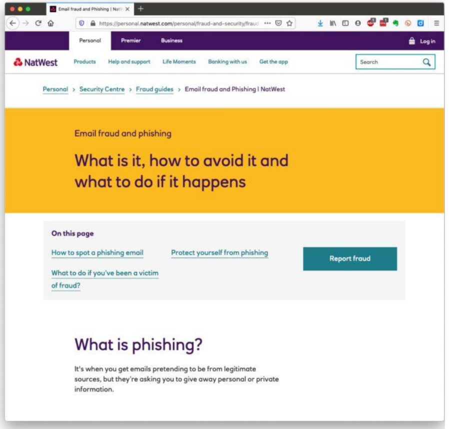
Working with cyber-security company Falanx Cyber, we scored 12 leading banks for the security of their online banking websites, looking at login security, encryption, account management, navigation and logout.

BANK	TEST SCORE
NatWest/Royal Bank of Scotland	83%
Nationwide	75%
Lloyds/Bank of Scotland/Halifax	74%
HSBC	73%
Barclays	73%
Tesco Bank	72%
First Direct	70%
Yorkshire Bank/Clydesdale Bank	68%
Santander	59%
Metro Bank	57%
The Co-operative Bank	56%
TSB	50%

Generally the big banks have got their online banking systems pretty secure and increasingly they're adding things like Two-factor authentication (2FA) to their systems to add increased levels of security.

Surprisingly (however it might seem) it's actually safer (more secure) to use a mobile phone app to contact your bank, or do online retailing than use your browser. This is because increasingly the app has 2FA baked into it, eg Touch ID, or FaceID on the iPhone. [***But only use over secure WiFi, or cellular***.]

This holds true for shopping as well. The major stores have adopted 2FA, or something like it, to protect your identity.



Personal › Security Centre › Fraud guides › Email fraud and Phishing | NatWest

Email fraud and phishing

What is it, how to avoid it and what to do if it happens

On this page

How to spot a phishing email

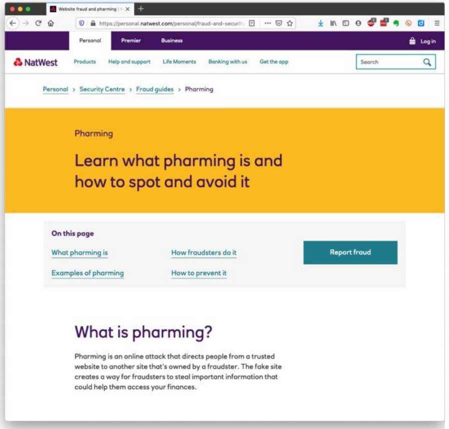
Protect yourself from phishing

What to do if you've been a victim of fraud?

Report fraud

What is phishing?

It's when you get emails pretending to be from legitimate sources, but they're asking you to give away personal or private information.



Personal › Security Centre › Fraud guides › Pharming

Pharming

Learn what pharming is and how to spot and avoid it

On this page

What pharming is

How fraudsters do it

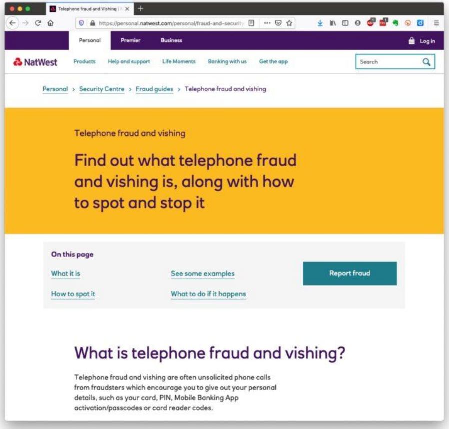
Examples of pharming

How to prevent it

Report fraud

What is pharming?

Pharming is an online attack that directs people from a trusted website to another site that's owned by a fraudster. The fake site creates a way for fraudsters to steal important information that could help them access your finances.



Personal › Security Centre › Fraud guides › Telephone fraud and vishing

Telephone fraud and vishing

Find out what telephone fraud and vishing is, along with how to spot and stop it

On this page

What it is

See some examples

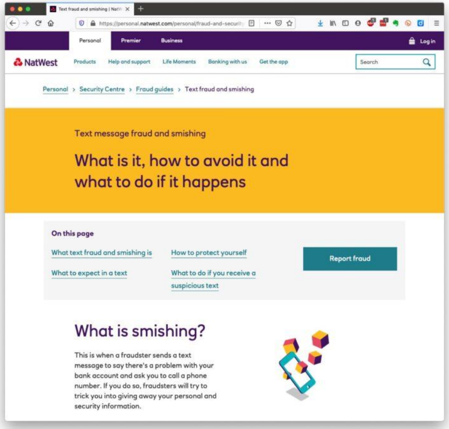
How to spot it

What to do if it happens

Report fraud

What is telephone fraud and vishing?

Telephone fraud and vishing are often unsolicited phone calls from fraudsters which encourage you to give out your personal details, such as your card, PIN, Mobile Banking App activation/passcodes or card reader codes.



Personal › Security Centre › Fraud guides › Text fraud and smishing

Text message fraud and smishing

What is it, how to avoid it and what to do if it happens

On this page

What text fraud and smishing is

How to protect yourself

What to expect in a text

What to do if you receive a suspicious text

Report fraud

What is smishing?

This is when a fraudster sends a text message to say there's a problem with your bank account and ask you to call a phone number. If you do so, fraudsters will try to trick you into giving away your personal and security information.

Who thinks up these names - phishing, pharming, vishing and smishing

What you can be sure of is that there are an awful lot of people trying to get hold of your identity, and it's down to YOU, and only YOU to stop them!

Your bank will have a set of pages, much like these, but for reference here's a couple of links …

Security Centre | Protect Yourself from Scams - NatWest (as above)

Internet Security Center - Norton

Another couple of demos …

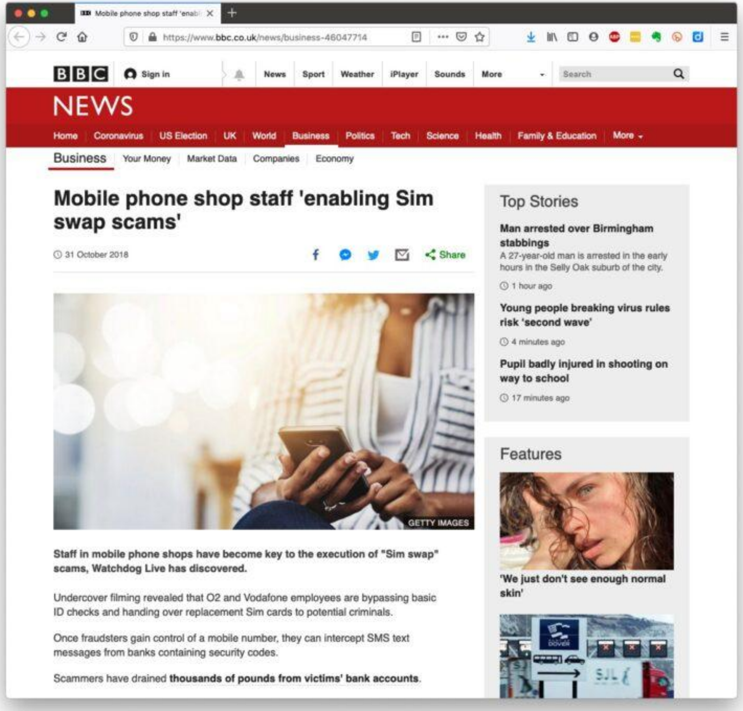
Take Five - To Stop Fraud

… and then some action …

Five ways to reset your relationship with your phone

Four things you can do today to protect your computer

… and then there's SIM card hacking …



Mobile phone shop staff 'enabling Sim swap scams'

31 October 2018

Staff in mobile phone shops have become key to the execution of "Sim swap" scams, Watchdog Live has discovered.

Undercover filming revealed that O2 and Vodafone employees are bypassing basic ID checks and handing over replacement Sim cards to potential criminals.

Once fraudsters gain control of a mobile number, they can intercept SMS text messages from banks containing security codes.

Scammers have drained **thousands of pounds from victims' bank accounts**.

Top Stories

Man arrested over Birmingham stabbings
A 27-year-old man is arrested in the early hours in the Selly Oak suburb of the city.
1 hour ago

Young people breaking virus rules risk 'second wave'
4 minutes ago

Pupil badly injured in shooting on way to school
17 minutes ago

Features

'We just don't see enough normal skin'

Mobile phone shop staff 'enabling Sim swap scams'

This one is a bit close to home, just to prove that all of us can be open to a well-planned scam.

A family member was caught by a SIM swapping event which I wrote up here …

Identity Theft – Thought grazing

… there's more about other SIM scams here …

3 Ways Your SIM Card Can Be Hacked (And How to Protect It) Your SIM card

… worrying but preventable in most cases.

Questions?

We’ve all got stories about scams, identity theft, does anyone want to share an experience?

Part 3: Measures to protect yourself

Let’s start at the very beginning - YOU!

As described above in the case of the SIM swap incident - take your time; don’t assume that because something appears to come from someone you might have got a message from, that is it from them.

Were you expecting a delivery - no … it’s a scam?

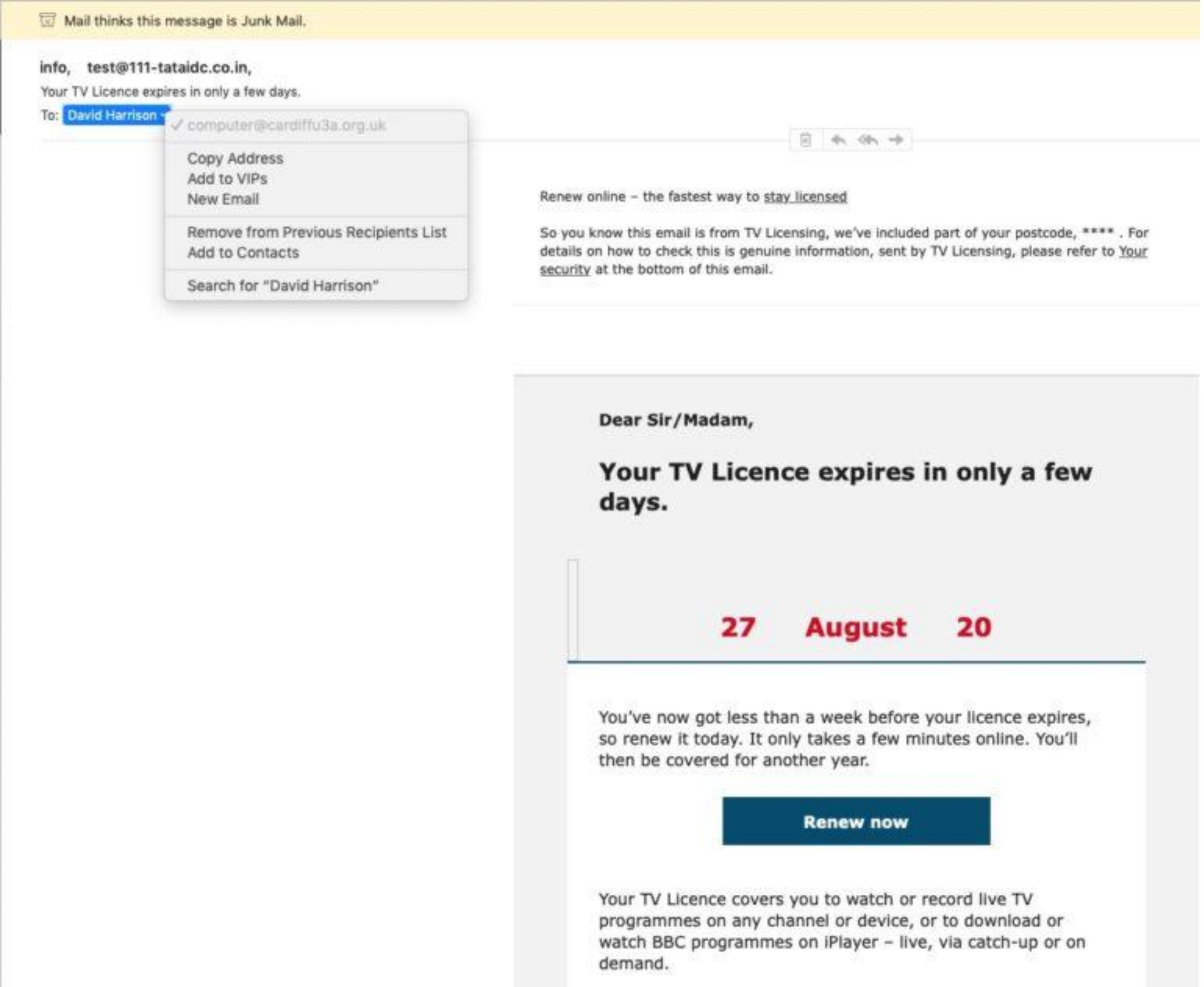
Is there something strange about the grammar in the message, or the way you’re being addressed?

Just remember if something seems to be good to be true, then it probably is too good to be true.

Check the Email headers (hover and examine from and to addresses).

Check the Web link (hover over it).

Check the mobile phone number (just type it in to your browser).



Mail thinks this message is Junk Mail.
✓ computer@cardiffu3a.org.uk
Copy Address
Add to VIPs
New Email
Remove from Previous Recipients List
Add to Contacts
Search for "David Harrison"
Renew now

info, test@111-tataidc.co.in,

Your TV Licence expires in only a few days.

To: David Harrison

Renew online – the fastest way to stay licensed

So you know this email is from TV Licensing, we've included part of your postcode, **** . For details on how to check this is genuine information, sent by TV Licensing, please refer to Your security at the bottom of this email.

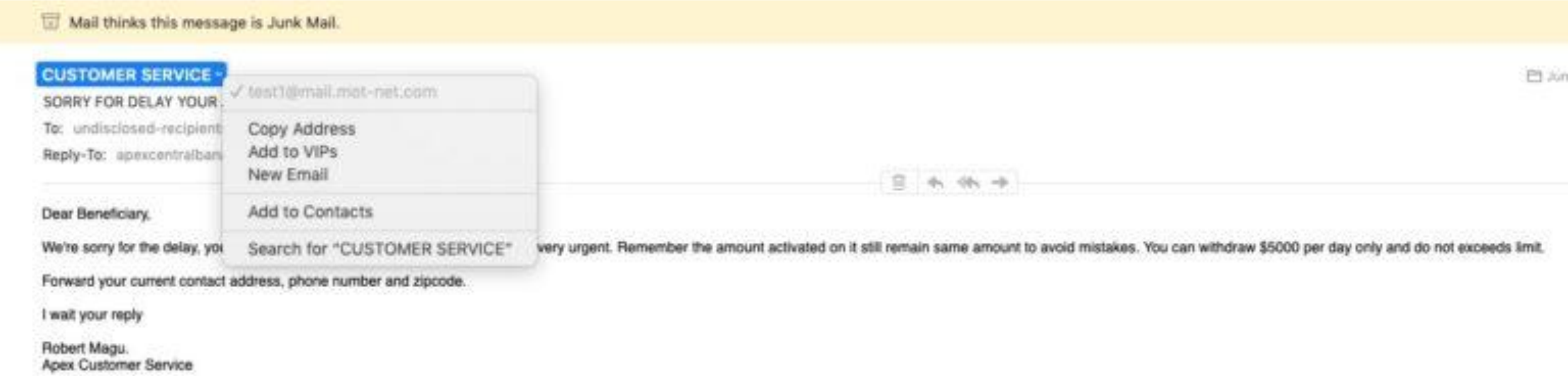
Dear Sir/Madam,

Your TV Licence expires in only a few days.

27 August 20

You've now got less than a week before your licence expires, so renew it today. It only takes a few minutes online. You'll then be covered for another year.

Your TV Licence covers you to watch or record live TV programmes on any channel or device, or to download or watch BBC programmes on iPlayer – live, via catch-up or on demand.



CUSTOMER SERVICE

SORRY FOR DELAY YOUR

To: undisclosed-recipient

Reply-To: apexcentralban

Dear Beneficiary,

We're sorry for the delay, yo very urgent. Remember the amount activated on it still remain same amount to avoid mistakes. You can withdraw $5000 per day only and do not exceeds limit.

Forward your current contact address, phone number and zipcode.

I wait your reply

Robert Magu.
Apex Customer Service

Hints and tips - 1

- Keep your operating software up to date. This is particularly true if you’re a Windows user, and even more true if you are still running an older version of Windows than Windows 10. If you’re using Windows XP, Windows Vista or even Windows 7 you should seriously consider disconnecting your machine from the internet.
- Install anti-malware, or anti-virus software if you’re a Windows user. Don’t pay more than you need to. Windows Defender from Microsoft is Free and for us relatively undemanding users more than sufficient. Keep it up-to-date as well! [*Your bank might be offering free software as well*.]
- Keep the software you use regularly up to date as well. Consider removing any software from your machine you don’t use – this is because software vulnerabilities are discovered sometimes quite a while after the software was first released.

Hints and tips - 2

❏ Be cautious over installing extensions into your browser. These are often extremely useful and valuable tools, ie password managers, Dropbox, note taking, Google Backup and Sync, but if you don’t get them from the official sources then you might be importing vulnerabilities, eg spyware and trojans to your system.

❏ Very seriously consider logging-out from social media and other retail sites when you've finished using them, especially Facebook, you just don't know what tracking and logging of what you do, even where you are, if you're logged in on a mobile device.

❏ Free software is both a boon and a curse. Only download open source software from a reputable site such as Softpedia, and **never try and get proprietary software for free**.

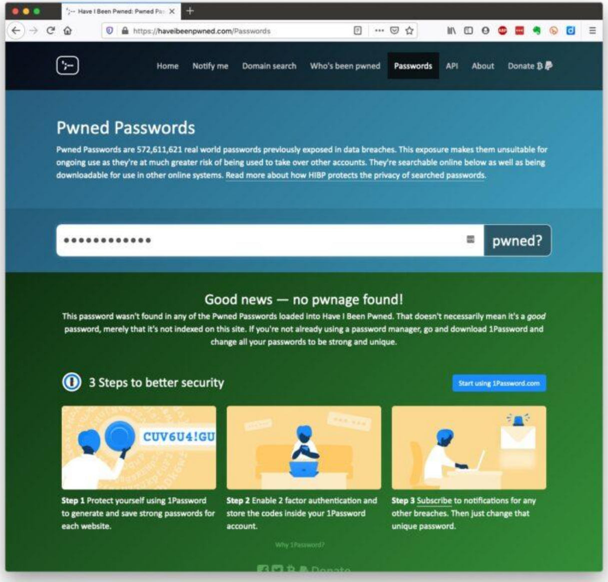
❏ Remember the golden rule 1 – if it seems too good to be true, it probably is, so steer clear!

❏ Remember the golden rule 2 – don’t speak to strangers (an oldie but goldie one, that); in other words if you don’t know where an email has come from – ignore it; if the website address looks a little strange – do an internet search on the company or organisation to check if the address you’re looking at is a spoof of the proper one.

Hints and tips - 3

- ❏ Have more than one email address. Use one as your personal address, other ones you can use to “throw away” when you need to register to a website, but you’re unlikely ever to go back to it again.
- ❏ Seriously consider using an email service that is NOT connected to your Internet Service Provider (ISP) – if you decide to change your ISP, and you should review them periodically, then you will have real problems if your email address is linked to their service!
- ❏ You’ve got Spam filters running? Of course you have. Probably your ISP, or email provider (eg Gmail, Yahoo, Microsoft Outlook or Hotmail) is filtering out what it thinks is spam, but occasionally some gets through. If that’s the case then you can always look at the real sender of your message.
- ❏ Check your Password is sound and secure
- ❏ Check your email address isn’t on a database of known data breaches
- ❏ Consider using a Password Manager - eg LastPass

… did I mention Passwords?



Pwned Passwords

Pwned Passwords are 572,611,621 real world passwords previously 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 systems. Read more about how HIBP protects the privacy of searched passwords.

•••••••••••••

Good news — no pwnage found!

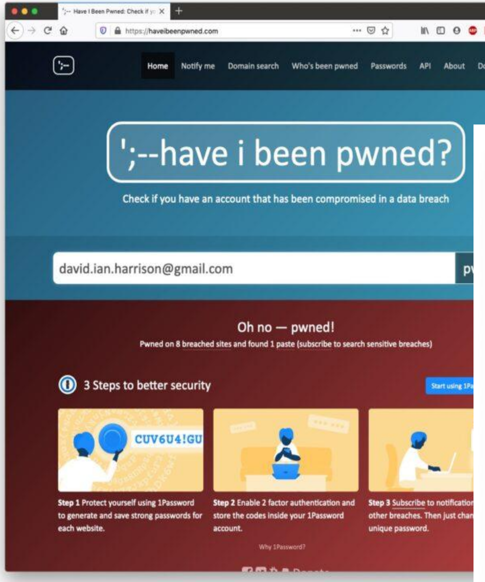
This password wasn't found in any of the Pwned Passwords loaded into Have I Been Pwned. That doesn't necessarily mean it's a *good* password, merely that it's not indexed on this site. If you're not already using a password manager, go and download 1Password and change all your passwords to be strong and unique.

3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.



Check if you have an account that has been compromised in a data breach

david.ian.harrison@gmail.com

Oh no — pwned!

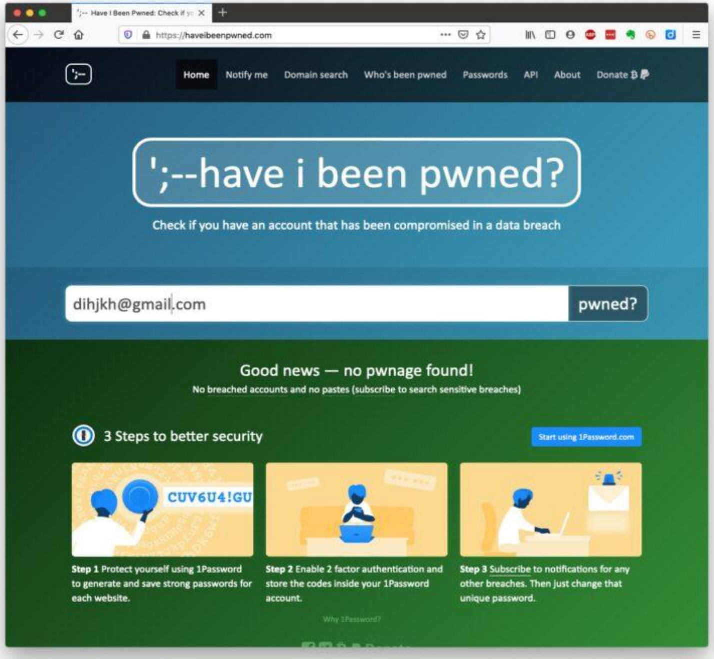
Pwned on 8 breached sites and found 1 paste (subscribe to search sensitive breaches)

3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notificatior other breaches. Then just char unique password.



Check if you have an account that has been compromised in a data breach

dihjkh@gmail.com

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

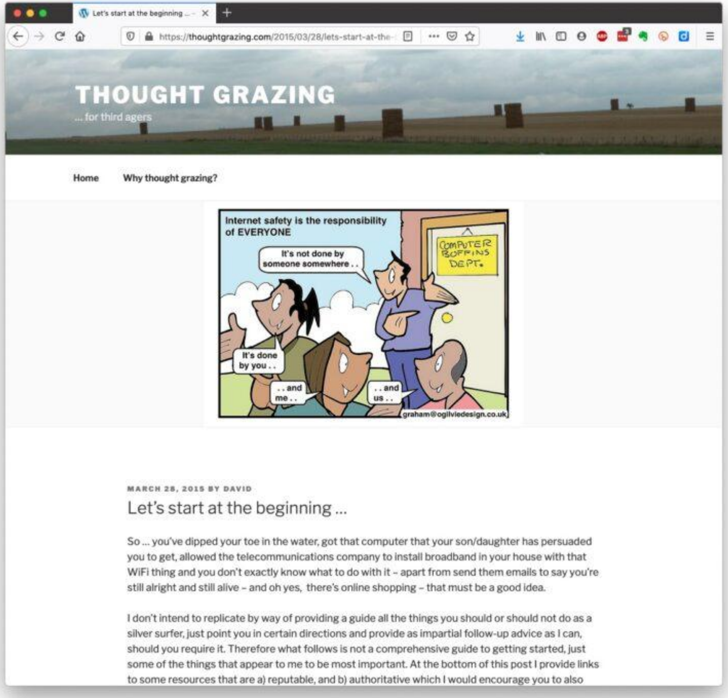
Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Pwned Passwords

Have I Been Pwned: Check if your email has been compromised in a data breach

Setting a secure password

Let's start at the beginning ... – Thought grazing



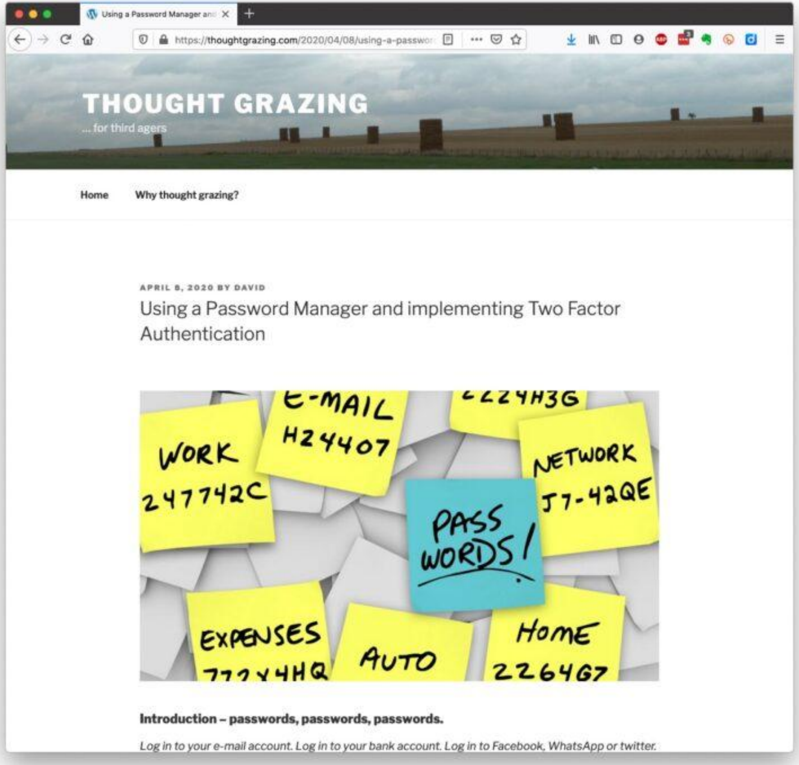
Let's start at the beginning ... –
https://thoughtgrazing.com/2015/03/28/lets-start-at-the-
THOUGHT GRAZING
... for third agers
Home
Why thought grazing?
Internet safety is the responsibility of EVERYONE
It's not done by someone somewhere . .
COMPUTER BOFFINS DEPT.
It's done by you . .
. . and me . .
. . and us . .
graham@ogilviedesign.co.uk

MARCH 28, 2015 BY DAVID

Let's start at the beginning ...

So ... you've dipped your toe in the water, got that computer that your son/daughter has persuaded you to get, allowed the telecommunications company to install broadband in your house with that WiFi thing and you don't exactly know what to do with it – apart from send them emails to say you're still alright and still alive – and oh yes, there's online shopping – that must be a good idea.

I don't intend to replicate by way of providing a guide all the things you should or should not do as a silver surfer, just point you in certain directions and provide as impartial follow-up advice as I can, should you require it. Therefore what follows is not a comprehensive guide to getting started, just some of the things that appear to me to be most important. At the bottom of this post I provide links to some resources that are a) reputable, and b) authoritative which I would encourage you to also



APRIL 8, 2020 BY DAVID

Using a Password Manager and implementing Two Factor Authentication

Introduction – passwords, passwords, passwords.

Log in to your e-mail account. Log in to your bank account. Log in to Facebook, WhatsApp or twitter.

Using a Password Manager and implementing Two Factor Authentication – Thought grazing

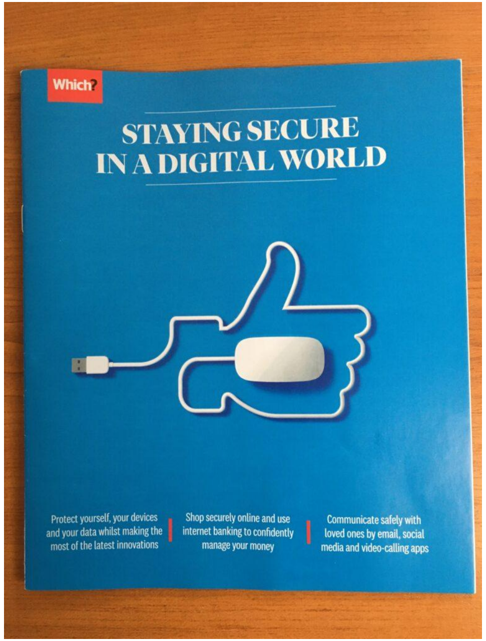
Final questions and links to close

Scams aimed at older people information - Which?

Scam Alert Service - Which?

Staying Safe in a Digital World - ageUK

Protect yourself from fraudsters | Fraud Guide - NatWest Bank



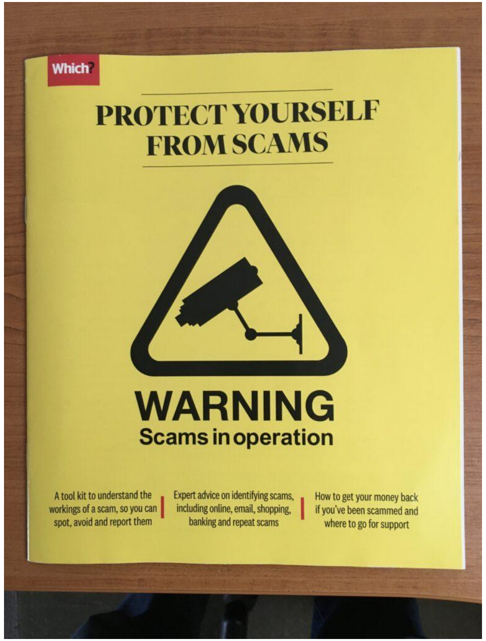
Which?

STAYING SECURE
IN A DIGITAL WORLD

Protect yourself, your devices and your data whilst making the most of the latest innovations

Shop securely online and use internet banking to confidently manage your money

Communicate safely with loved ones by email, social media and video-calling apps



Which?

PROTECT YOURSELF
FROM SCAMS

WARNING
Scams in operation

A tool kit to understand the workings of a scam, so you can spot, avoid and report them

Expert advice on identifying scams, including online, email, shopping, banking and repeat scams

How to get your money back if you've been scammed and where to go for support