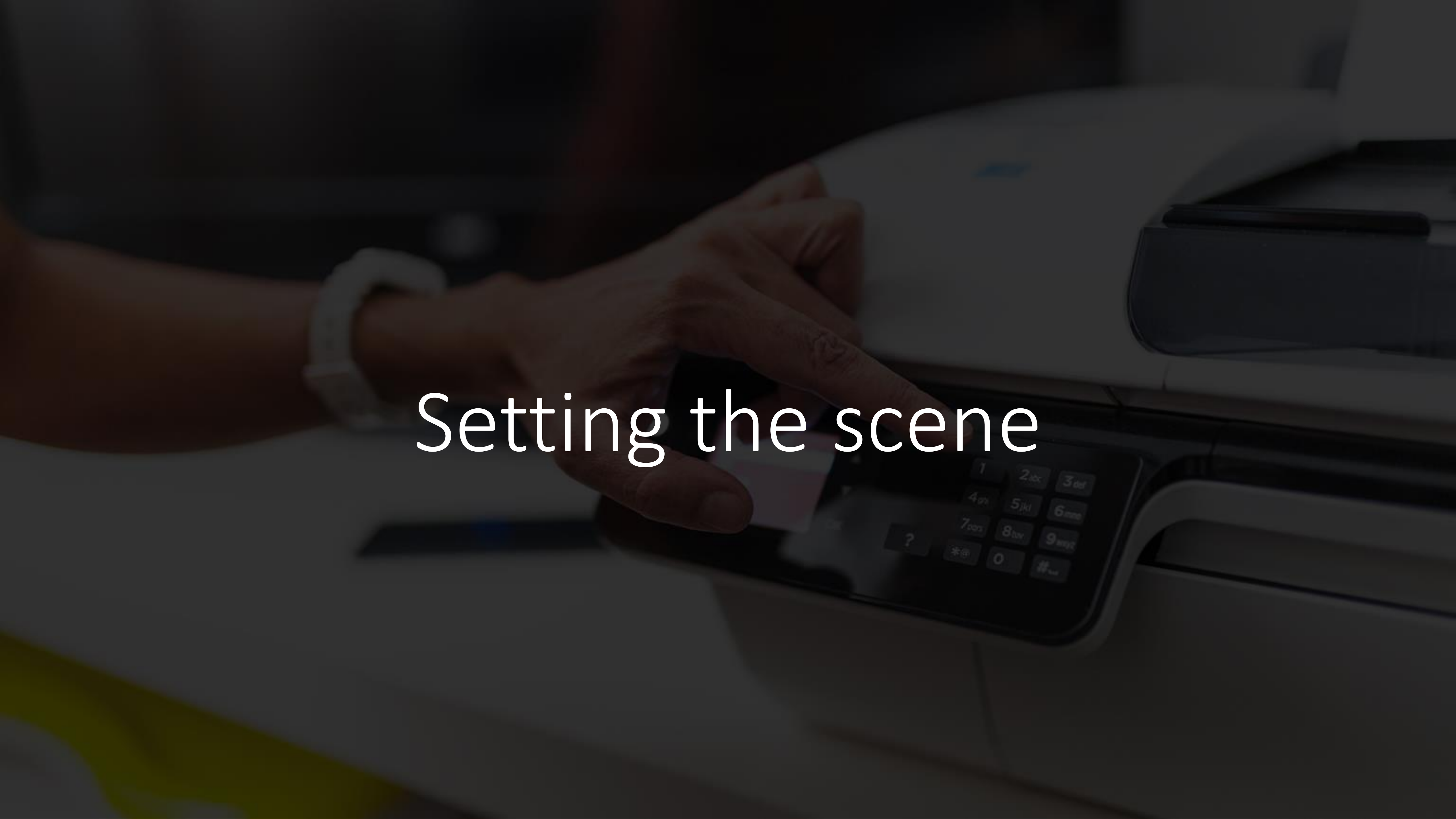
CYBER SCOTLAND WEEK 2020 17-23 FEB

Staying secure online

Robert Stewart
Scottish Social Services Council

Agenda

- Welcome
- Setting the scene
- How vulnerable are you to online threats?
- Tips to keep you safe
- Live simulation exercise and feedback
- What next?



Setting the scene

2019 SSSC cyber awareness survey

- **98%** of people said keeping safe online is a high priority to them. But only **22%** are taking adequate steps to protect themselves from common threats eg by using two-factor authentication.
- Only **9%** of respondents always use a password manager.
- **39%** of respondents do not always lock their computer screen when they step away from it
- **25%** of respondents do not consider keeping people, devices and information secure to be the responsibility of everyone within their organisation. **10%** of those surveyed believe it is solely the job of IT professionals and another **8.5%** managers.

2019 SSSC cyber awareness survey

- **61%** of respondents do not always install the latest software and app updates once they notice that they are available.
- **62%** of respondents do not always back up their most important data.
- **36%** of respondents have never had cyber security training in their workplace. Just **46%** received some sort of training within the last year.

How vulnerable are you ?

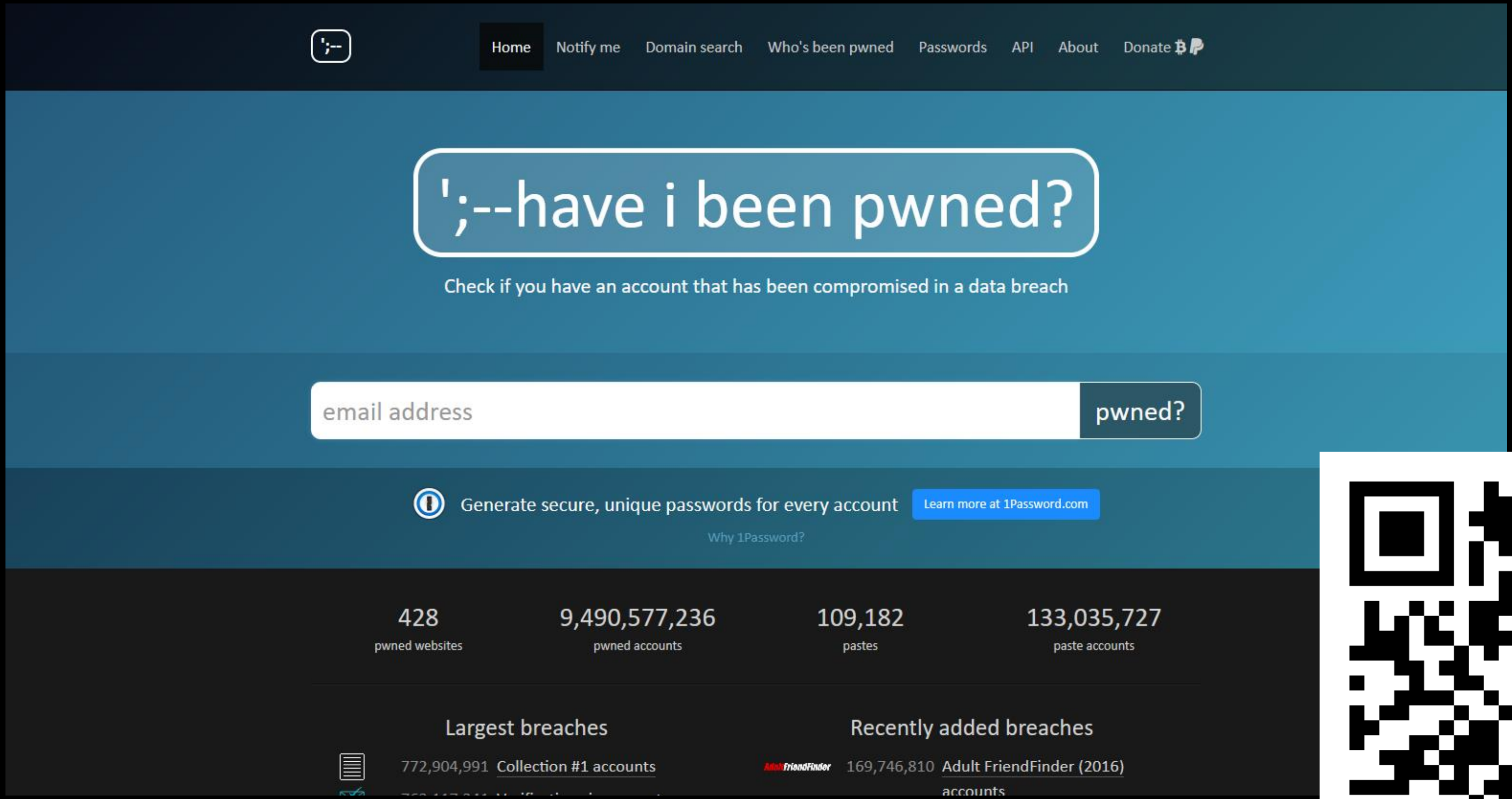
How vulnerable are you? Devices

Laptop	Desktop PC	Games console	Smartphone
Smart speaker	Tablet	IP camera	Landline
Router	Smart TV	Smart Thermostat	Smart Lightbulb

How vulnerable are you? Online accounts

- Social media
- Email
- Online banking
- Internet provider
- Online gaming websites
- Music streaming
- Internet TV
- MySSSC
- Mobile provider
- Apps
- Utility providers
- Online shopping

';--have i been pwned?



';--have i been pwned?

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

Generate secure, unique passwords for every account

428	9,490,577,236	109,182	133,035,727
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

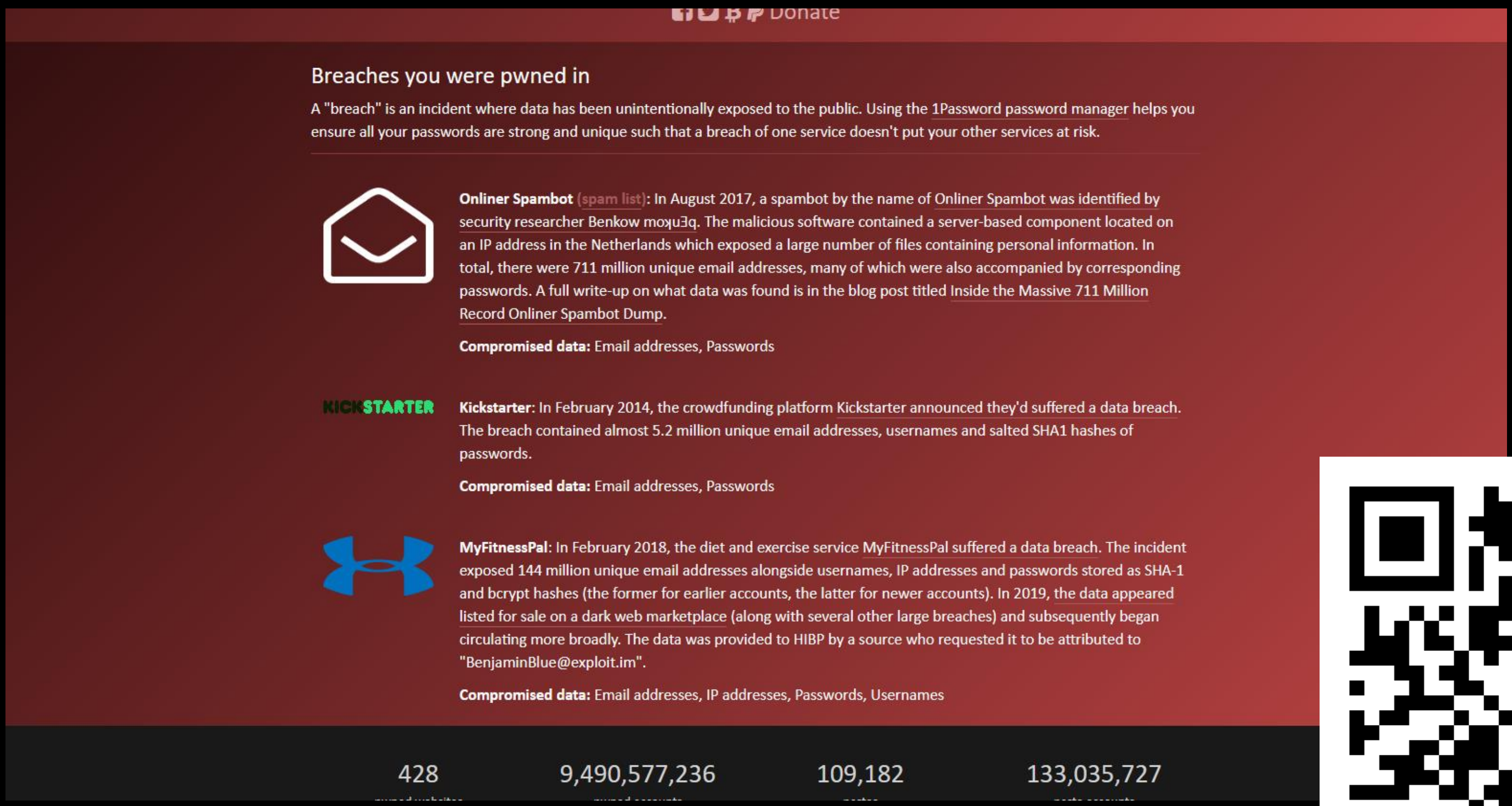
772,904,991 Collection #1 accounts

Recently added breaches

169,746,810 Adult FriendFinder (2016) accounts

www.haveibeenpwned.com

';--have i been pwned?



Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Onliner Spambot (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moʞuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

Kickstarter: In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

Compromised data: Email addresses, Passwords

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames

428 9,490,577,236 109,182 133,035,727

www.haveibeenpwned.com

Tips to keep you safe

Tips to keep you safe

Protecting your online accounts

Protecting your data

Protecting your devices

Protecting your online accounts

Passwords, password managers and two factor authentication

Question

Choose the strongest password from the options:

1. b*E2p&08
2. TasteYardsBoxed
3. 1q2w3e4r5t
4. Qwertyuiop
5. OneMilesTrunk
6. London2012

Question

Choose the strongest password from the options:

1. b*E2p&08 = 9 hours
2. TasteYardsBoxed = 44 million years
3. 1q2w3e4r5t = Instantly
4. Qwertyuiop = Instantly
5. OneMilesTrunk = 16 thousand years
6. London2012 = Instantly

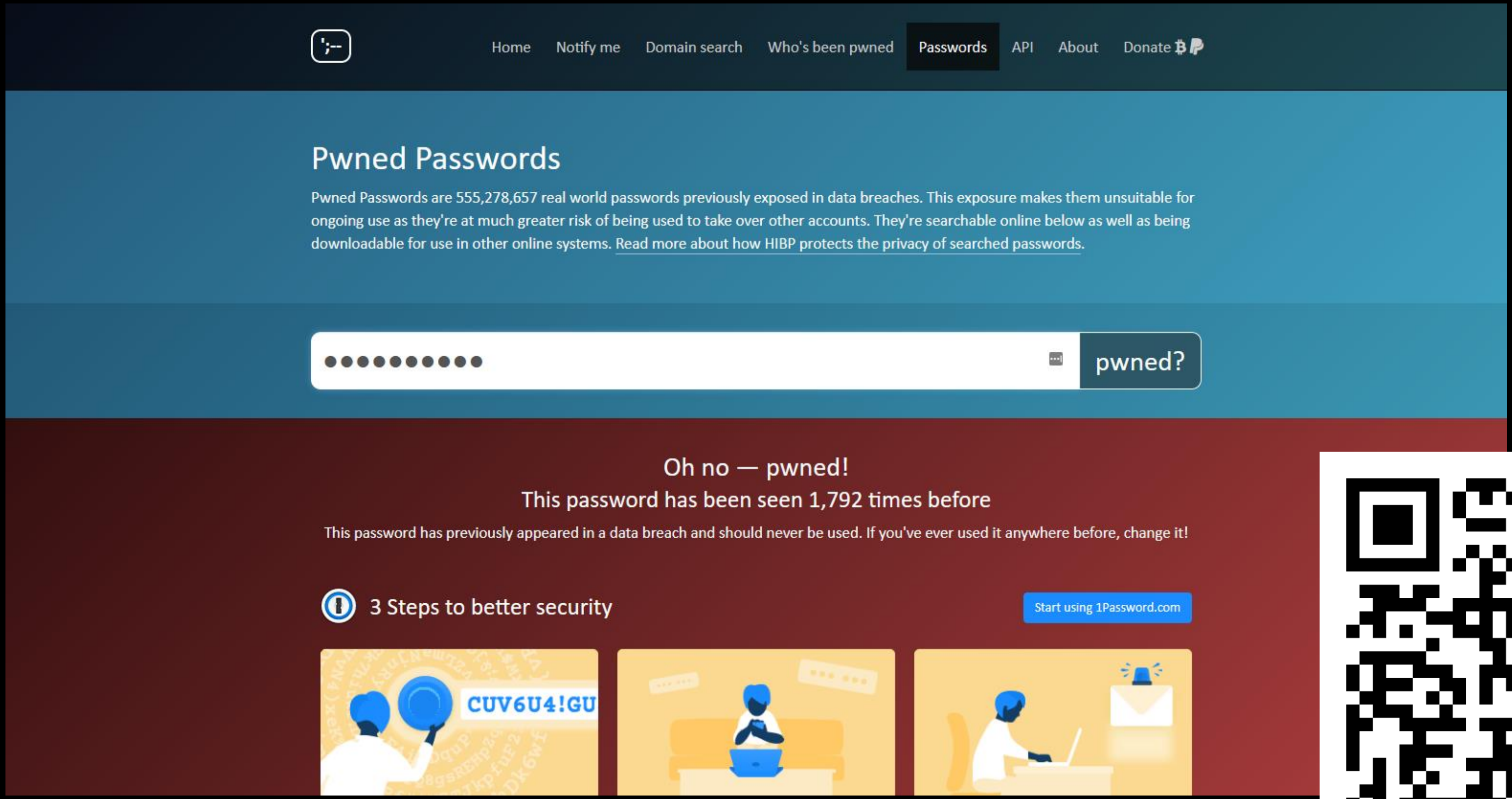
Use three or more random words. Make your passwords as long as possible.

National Cyber Security Centre guidance

You make it easier for someone to steal your password if you:

- Store your password in a word document or write it down somewhere it can be found.
- Use family members names as your password.
- Don’t change the default password.
- Use a common password like ‘123456’ or ‘Password’ as your password.
- Use the same password on multiple accounts.
- Add a number to the end of an old password.
- Share your password with someone.

How secure is my password?



Pwned Passwords

Pwned Passwords are 555,278,657 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.

●●●●●●●●●●● pwned?

Oh no — pwned!
This password has been seen 1,792 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

3 Steps to better security

Start using 1Password.com

haveibeenpwned.com/Passwords

Protect your email account by using a strong, separate password.

National Cyber Security Centre guidance

Never use the same password across multiple online accounts.

National Cyber Security Centre guidance

What if your passwords could look like this?

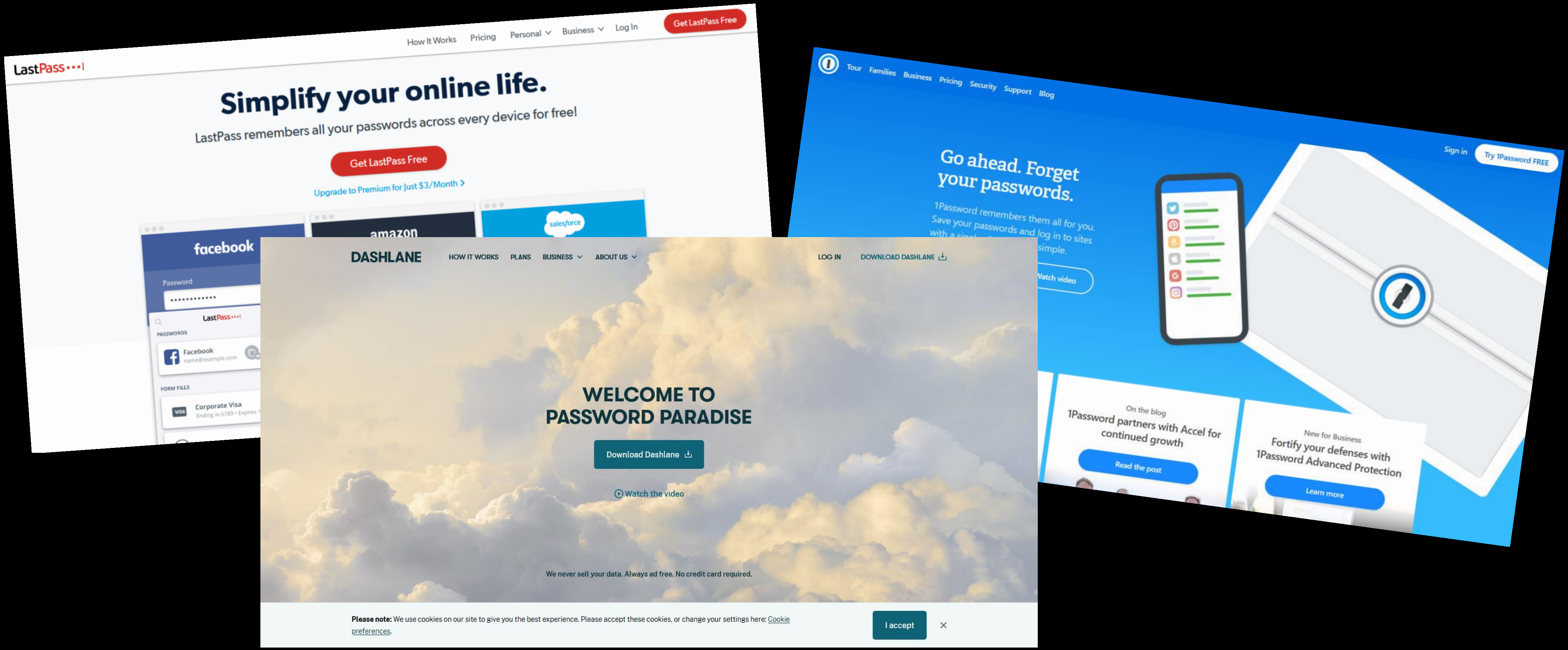
jT50xoiTUj!rwUV*5tQyaJ7%nN54Z0

What if your passwords could look like this?

jT50xoiTUj!rwUV*5tQyaJ7%nN54Z0

= 312 undecillion years

Password managers



Simplify your online life.

LastPass remembers all your passwords across every device for free!

WELCOME TO PASSWORD PARADISE

We never sell your data. Always ad free. No credit card required.

Please note: We use cookies on our site to give you the best experience. Please accept these cookies, or change your settings here: Cookie preferences.

Go ahead. Forget your passwords.

1Password remembers them all for you. Save your passwords and log in to sites with a sin simple.

On the blog

1Password partners with Accel for continued growth

New for Business

Fortify your defenses with 1Password Advanced Protection

“We know that we're supposed to create a unique, hard-to-guess password for all of our online accounts… However the NCSC recognise that this virtually impossible to do without help. Password managers provide that help.”

National Cyber Security Centre website
www.ncsc.gov.uk

2FA

Two Factor Authentication

Question

Choose the strongest method of 2FA from the list:

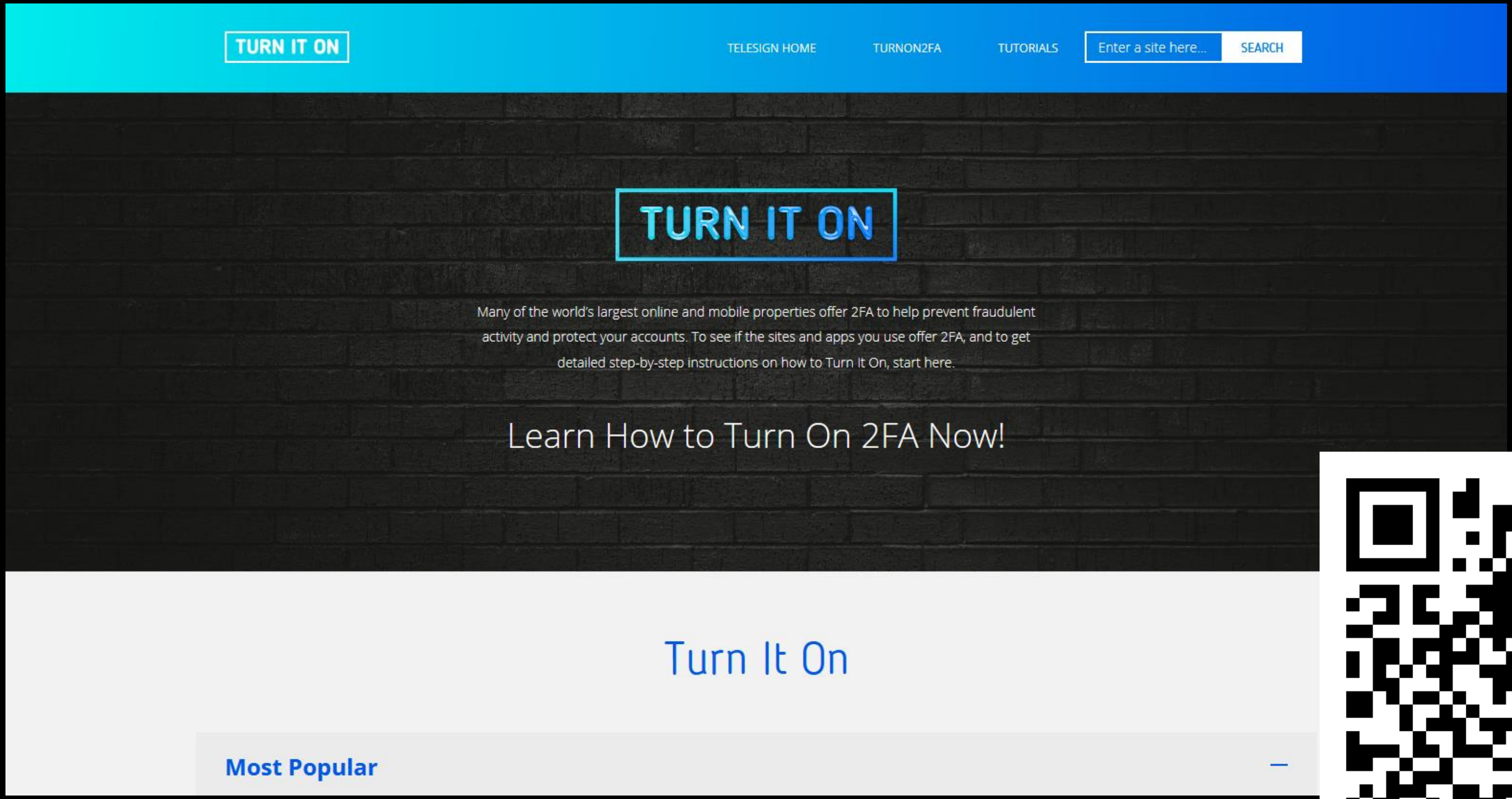
1. Text message to my mobile phone
2. Code generator app on my smartphone
3. Login verification link sent to my email
4. Yubikey or other U2F key
5. Nothing at all

Question

Choose the strongest method of 2FA from the list:

1. Yubikey or other U2F key
2. Code generator app on my smartphone
3. Text message to my mobile phone
4. Login verification link sent to my email
5. Nothing at all

Turn it on



Many of the world's largest online and mobile properties offer 2FA to help prevent fraudulent activity and protect your accounts. To see if the sites and apps you use offer 2FA, and to get detailed step-by-step instructions on how to Turn It On, start here.

Learn How to Turn On 2FA Now!

Turn It On

Most Popular

www.telesign.com/turnon2fa/tutorials

> 2FA is the single best thing you can do to improve the security of your important accounts.

National Cyber Security Centre guidance

Summary

- Three word passphrase
- Use a password manager
- Turn on 2FA

Protecting your data

Backups, encryption and data minimisation

Question

How often do you back up your important files?

1. Daily
2. Weekly
3. Monthly
4. Less often
5. Never

Question

How often do you test your backups to make sure they work?

1. Daily
2. Weekly
3. Monthly
4. Less often
5. Never

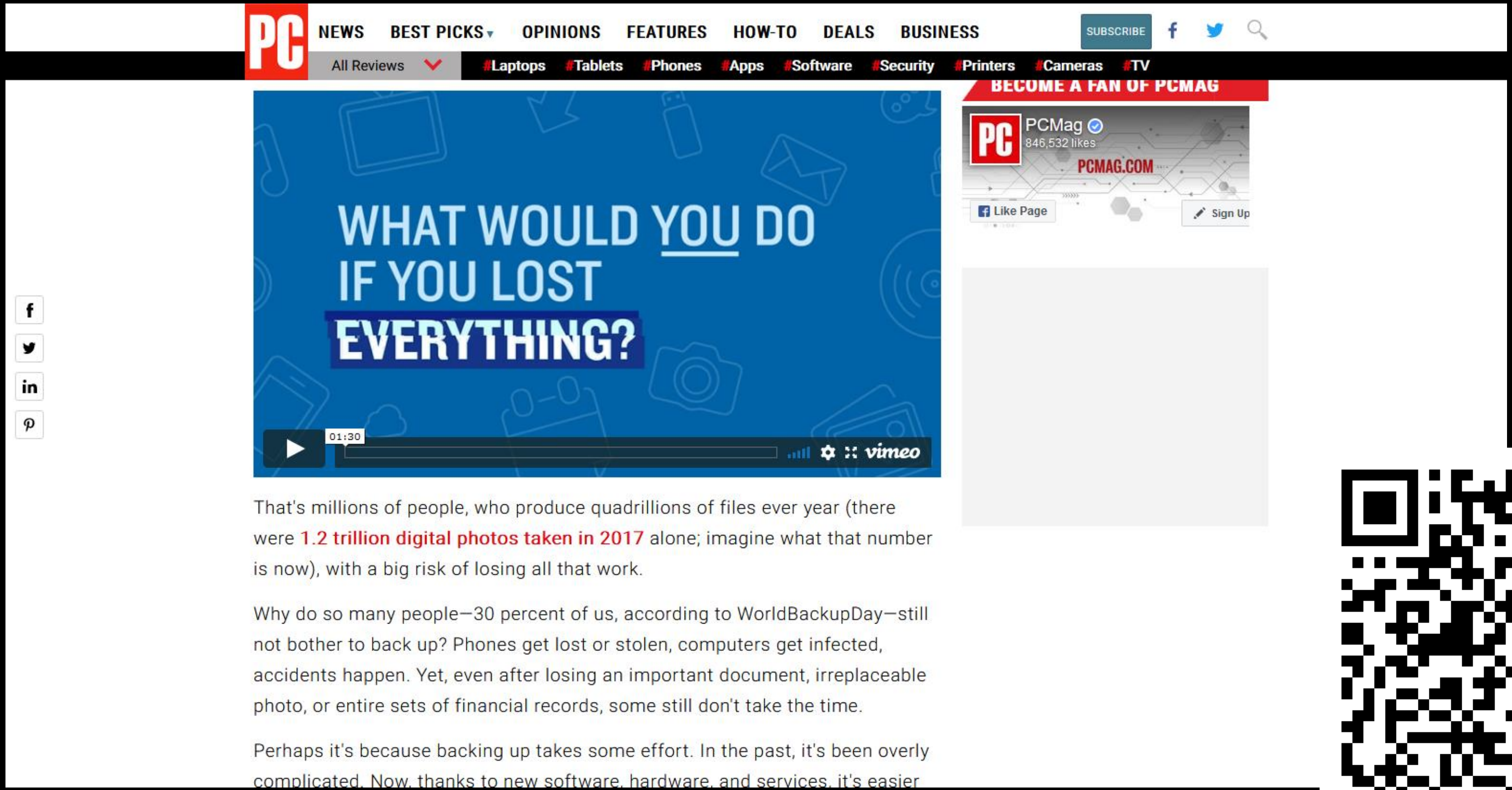
Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system

National Cyber Security Centre guidance

Make sure that the external hard drive you are using to back-up your data is not permanently connected to the device you are backing up either physically or over a local network connection.

National Cyber Security Centre guidance

How to backup



That's millions of people, who produce quadrillions of files ever year (there were 1.2 trillion digital photos taken in 2017 alone; imagine what that number is now), with a big risk of losing all that work.

Why do so many people—30 percent of us, according to WorldBackupDay—still not bother to back up? Phones get lost or stolen, computers get infected, accidents happen. Yet, even after losing an important document, irreplaceable photo, or entire sets of financial records, some still don't take the time.

Perhaps it's because backing up takes some effort. In the past, it's been overly complicated. Now, thanks to new software, hardware, and services, it's easier

uk.pcmag.com

Question

How often do you delete the contents of your email account?

1. Every six months
2. Every year
3. Every two years
4. When it gets full
5. Never

Delete what you no longer need (emails, accounts, posts, files) and significantly reduce your exposure to cyber crime. Prioritise sensitive data.

SSSC Staying Safe Online guidance

How much do strangers know about you?

Privacy settings and social media

Summary

- Backup regularly and test to make sure they work.
- Use encryption wherever you can.
- Minimise your data by deleting old data and using privacy settings.

Extra tips…

- Don’t use your devices in a public place where people can see what you are working on. Look out for reflections in windows etc.
- Never use public Wi-Fi to send or receive sensitive data. Use a Virtual Private Network (VPN).
- Don’t share your devices with others if you use them to perform sensitive tasks like online banking, checking your email etc. Use separate user accounts if you can’t avoid this.

Protecting your devices

Anti-malware software, updates and safe use

You need anti-malware software on Windows and MacOS devices

Windows Defender

PC status: Protected

Your PC is being monitored and

Real-time protection: On

Virus and spyware definitions: Up to date

Scan details

Last scan: Today at 7:27 AM (Quick scan)

You are protected

2013 build 2793

Bitdefender Total Security 2017

EVICE

ROTECTED

ATE UPDATE NOW

AUTOPILOT

OK, we got this

Security for home networks

Advice on choosing anti-malware

- Don’t rely solely on internet reviews. They are sometimes paid for.
- Look out for adverts posing as search listings.
- Choose something that is well known. Ask friends, family.
- Cyber security professionals test anti-malware software and post their results to YouTube. This can be a good source of information.

Install updates when they become available

Cyber criminals use weaknesses in software and apps to attack your devices and steal your identity. Software and app updates are designed to fix these weaknesses and installing them as soon as possible will keep your devices secure.

National Cyber Security Centre guidance

You’ll often receive a prompt on your computer, smartphone or tablet to inform you that a software or app is ready to be updated. Don’t ignore this message.

National Cyber Security Centre guidance

Advice on safe use

- Avoid high risk websites or software.
- Regularly delete temporary files, cookies etc.
- Use an ad-blocker when browsing the web. Even legitimate websites can infect your computer with malware through their ad networks.
- Only install software you absolutely need and uninstall anything you no longer use.
- Avoid ‘living in your admin account’. Create a normal user account to login with and only login as an admin when you need to.

Question

You are downloading a new app onto your smartphone. Which of the following will give you confidence that the app has a good reputation?

1. It has many positive comments/reviews
2. It has a high install count eg 10m+ installs
3. It has five stars
4. You already know people who use it
5. The name of the company offering the app is well known
6. You have found the app via the official website of a company

Summary

- Install anti-malware software and keep it updated.
- Always install software and app updates when they become available. Set them to auto-update if you like, but check they update.
- Follow our advice on safe use to avoid the most common threats.

Simulation

Service A

Incident one

Monday 8am. You are the service manager.

Jess, one of the office administrators, asks if the gift card codes she sent you were what you were looking for. You have no idea what she is talking about.

- Jess says she received an email from you on Saturday morning.
- The email asked her to purchase £200 of gift cards for a raffle.
- The email said these were required immediately and she could claim the money back instantly on expenses.
- She bought gift vouchers on Amazon and responded to the email with the voucher codes.

Incident two

Tuesday 3pm

The eLearning provider used by the service sends out an email to say there has been a data breach involving their service.

- Usernames, email addresses, passwords and telephone numbers have been disclosed.
- The passwords were not hashed.
- The provider says that it takes security very seriously and has improved security following the breach. It recommends people change their password when they next login.

Incident three

Wednesday 9am

You learn that Andrew, a senior member of staff, has sent out thousands of emails to people inside and outside the organisation. Each email advertised pharmaceutical websites and an ‘anti-aging’ treatment.

- Complaints are flooding into the service’s enquiries team.
- Andrew denies sending these emails.
- Andrew uses Office 365 email.
- Your IT provider says sensitive files Andrew had access to have been accessed and possibly copied.

Incident four

Thursday 10am

You are notified that the services website has been hacked. All links on the website redirect visitors to pornography. Nobody knows how to fix the website, but you need to do something quickly as it has been noticed by people who use the service.

- The member of staff who built the website no longer works here.
- The website uses the Wordpress CMS.
- The software has not been updated since the person left.
- Nobody knows where the website is hosted or who to contact.

Incident five

Friday 2pm

Over lunch all of computers in the service begin to stop working. They show a message stating that files have been encrypted and that you must pay a ransom to decrypt them.

- Files on the shared drive have also been encrypted.
- Work has ground to a halt.
- Attempts overnight by your IT provider to recover the files fails after the backups are discovered to be faulty.

Service B

Incident one

Monday 2pm. You are the service manager.

You return from lunch to find the deputy manager is on the phone to BT. She looks worried. She tells you that someone has been trying to hack into the service’s internet connection and BT are fixing it for her now.

- She was alerted to this by a call from BT.
- The caller asked to connect to her laptop to fix the issue.
- They are also connected to the desktop PC.

Incident two

Wednesday 5pm

You try to login to the service’s email account but it asks you for a 2-step verification code. You haven’t set this up and you don’t recognise the last digits of the mobile number it says the code has been sent to.

- Other staff say they can’t login either and nobody has setup 2-step verification on this account.

- You begin to receive phone calls from people who use the service. They are angry to have been sent emails demanding payment.

- Further calls come in from stakeholders warning that you are emailing malware out to people. You still have no access to your email account.

Incident three

Thursday 11am

The deputy manager tells you that she has lost her laptop. She left it on the luggage rack of the bus and it was taken by someone, either deliberately or by mistake.

- The laptop’s hard disk is not encrypted.
- There is a password on the user account. But will this keep the data safe?
- Returns for the Care Inspectorate were stored on this laptop and only older versions of the files are held on the USB backup.
- The service’s USB backup was attached to the device when it was stolen.

Incident four

Saturday 9am

Most of the staff have had their Facebook and Instagram accounts hacked overnight. Some even lost access to their email accounts.

- Only staff from this service seem to be affected.
- The affected staff are frequent users of the desktop PC in the office or have used it within the last month.
- •The impact on staff has been devastating. Many have lost photos and messages stored on their social media accounts and keep no other copies of these.

Incident five

Sunday 2pm

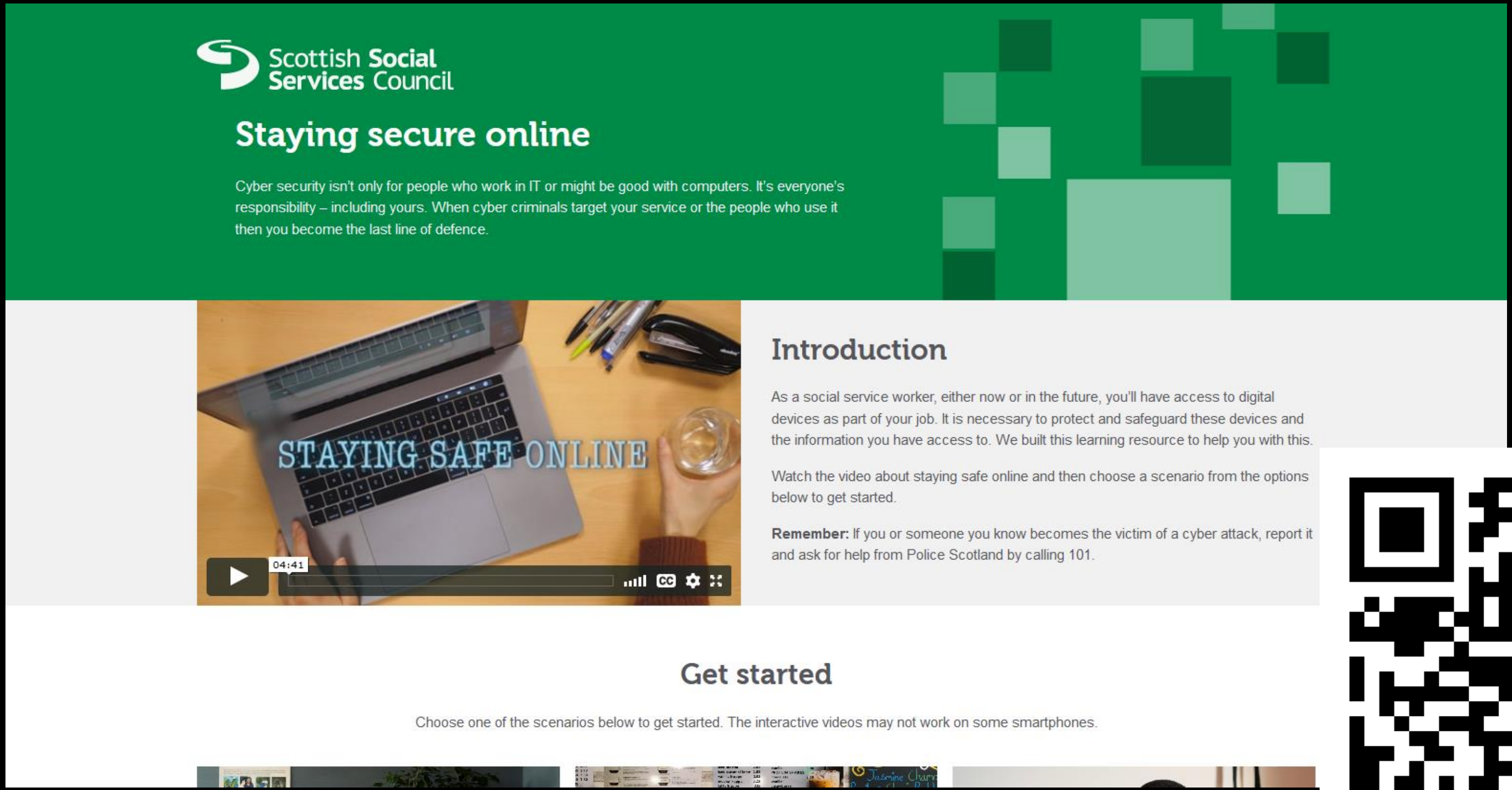
You examining the services bank statements following notice from your landlord that they have not been paid rent for the month. The bank statement shows that they have been paid, although you do not recognise the account number.

- A member of staff recently updated the payee details following an email from the landlord.
- The email appears legitimate and shows no sign of being a phishing email. You forward it on the landlord.
- The landlord says the headers of the email show it was not sent by them, even though the sender and sender's email look like it did.

What next?

CYBER SECURITY
built for maximum security and protect important
records and valuables against fire
SAFE
SAFE
Please Enter OTP
7 6 2 8 3 5
OTP ID: 7EUA GF6E YU26
10 second left
Send OTP

Staying secure online from SSSC



Scottish Social Services Council

Staying secure online

Cyber security isn't only for people who work in IT or might be good with computers. It's everyone's responsibility – including yours. When cyber criminals target your service or the people who use it then you become the last line of defence.

Introduction

As a social service worker, either now or in the future, you'll have access to digital devices as part of your job. It is necessary to protect and safeguard these devices and the information you have access to. We built this learning resource to help you with this.

Watch the video about staying safe online and then choose a scenario from the options below to get started.

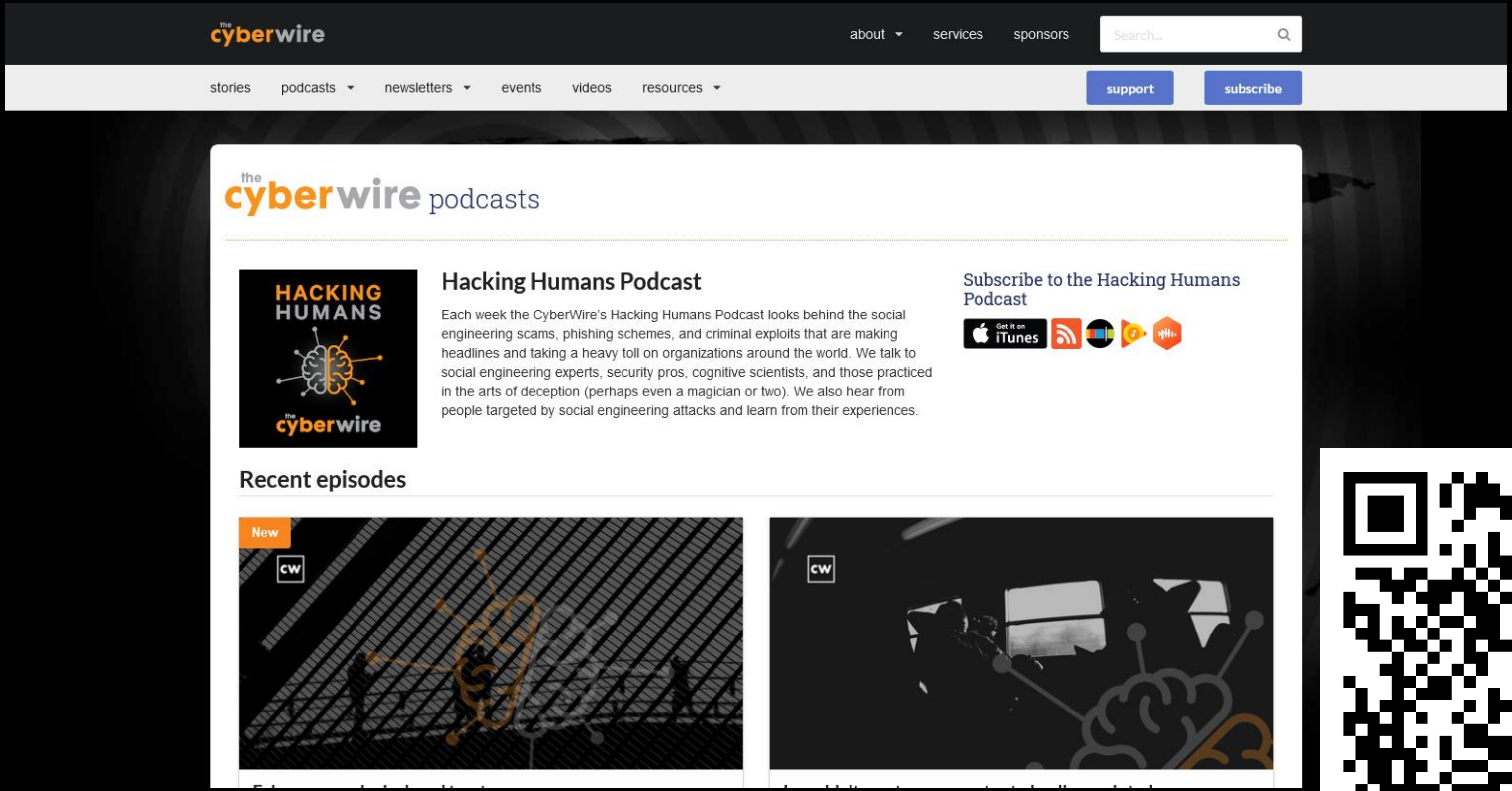
Remember: If you or someone you know becomes the victim of a cyber attack, report it and ask for help from Police Scotland by calling 101.

Get started

Choose one of the scenarios below to get started. The interactive videos may not work on some smartphones.

learn.sssc.uk.com/cyber

Hacking Humans podcast from CyberWire



Hacking Humans Podcast

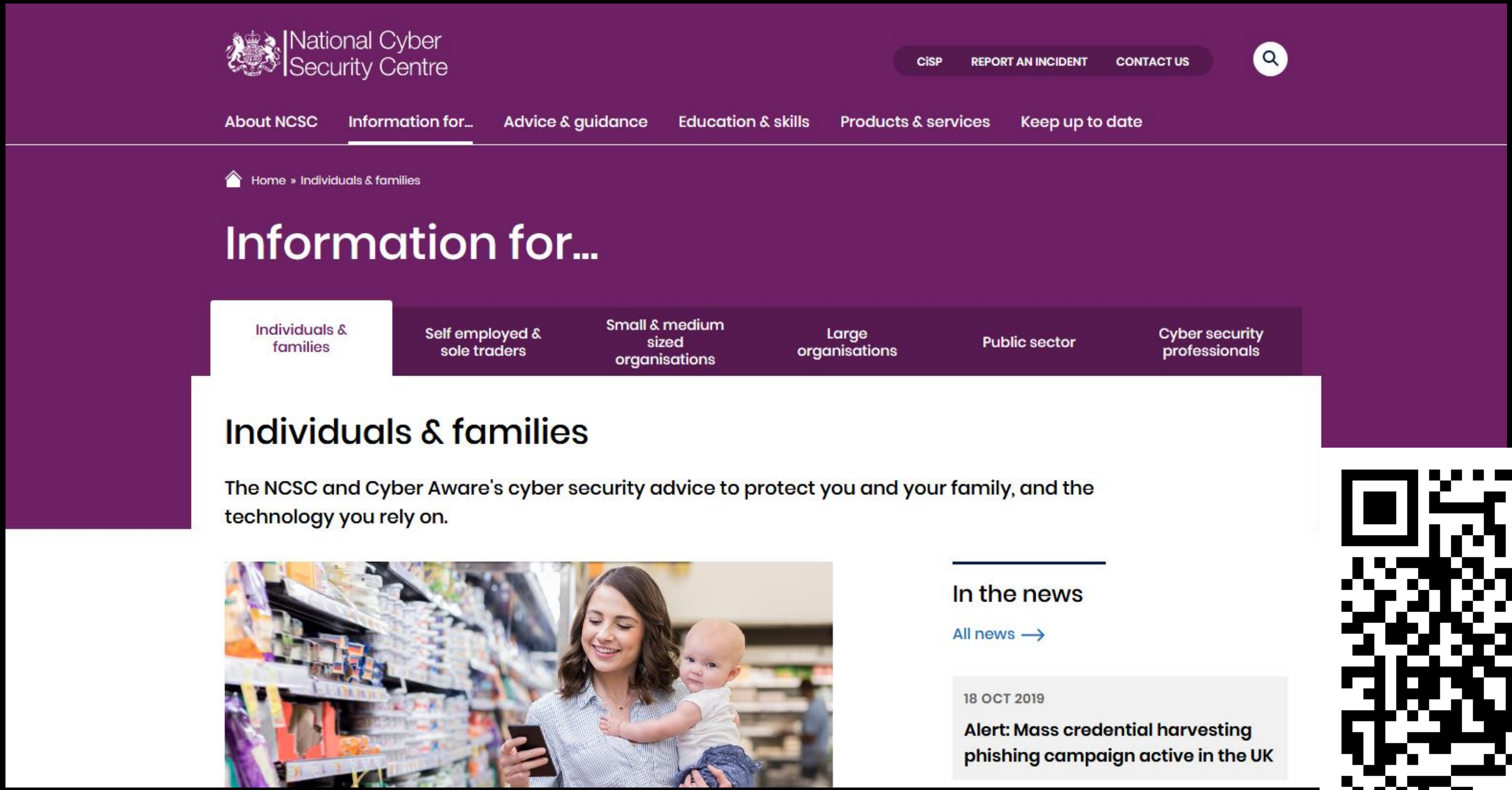
Each week the CyberWire's Hacking Humans Podcast looks behind the social engineering scams, phishing schemes, and criminal exploits that are making headlines and taking a heavy toll on organizations around the world. We talk to social engineering experts, security pros, cognitive scientists, and those practiced in the arts of deception (perhaps even a magician or two). We also hear from people targeted by social engineering attacks and learn from their experiences.

Subscribe to the Hacking Humans Podcast

Recent episodes

thecyberwire.com

National Cyber Security Centre



National Cyber Security Centre

CiSP REPORT AN INCIDENT CONTACT US

About NCSC | Information for... | Advice & guidance | Education & skills | Products & services | Keep up to date

Home » Individuals & families

Information for...

Individuals & families | Self employed & sole traders | Small & medium sized organisations | Large organisations | Public sector | Cyber security professionals

Individuals & families

The NCSC and Cyber Aware's cyber security advice to protect you and your family, and the technology you rely on.

In the news

All news ⟶

18 OCT 2019

Alert: Mass credential harvesting phishing campaign active in the UK

www.ncsc.gov.uk

Thank you

CYBER 17-23 FEB SCOTLAND WEEK2020

- Find out more at **learn.sssc.uk.com/cyber**
- Email any questions to **sssclearningtech@sssc.uk.com**
- One session is not enough to cover everything you need to know. Please commit yourself to finding our more about staying secure online.

If you or someone you know becomes the victim of a cyber attack, report it and ask for help from Police Scotland by calling 101.