PROTECTING YOUR COUNCIL, YOUR RESIDENTS AND YOURSELF FROM CYBERCRIME

Cyber Security Advisor - John Greenwood

💡 = *Thinking point.*

NS Cyber Crime Unit

POLICE
NORFOLK & SUFFOLK
working together for you

NSCYBER

Cyber *dependant* crimes

- **Pursue** - Investigation
- CHOICES - Stop Involvement
- **Protect** - Increase Defence
- **Prepare** - Increase Resilience

Cyber Enabled

- 'traditional crimes', which can be increased in their scale or efficiency by use of computers / ICT

  - *Fraud / Credit card theft*
  - *Investment Scams*
  - *Romance Scams*

Cyber Dependent

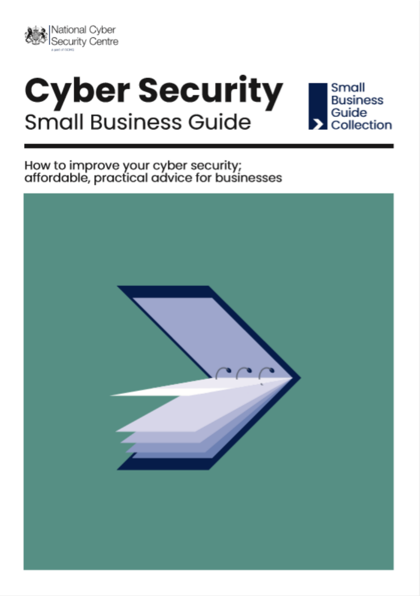
- Offences that can only be committed using a computer / ICT

  - *Malware (viruses, ransomware)*
  - *Hacking*

National Cyber Security Centre

a part of GCHQ

- Provides a single point of contact for individuals and organisations of all sizes in relation to cyber security

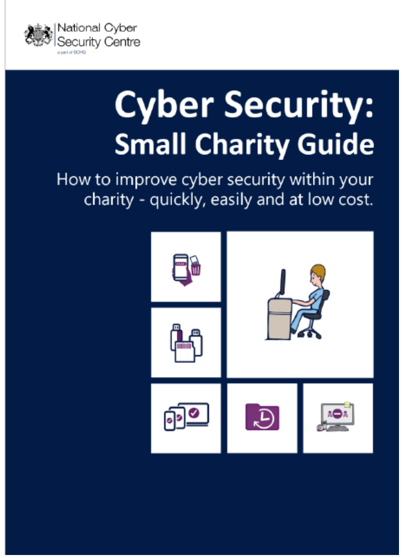


National Cyber Security Centre

Cyber Security
Small Business Guide

Small Business Guide Collection

How to improve your cyber security; affordable, practical advice for businesses



National Cyber Security Centre

Cyber Security: Small Charity Guide

How to improve cyber security within your charity - quickly, easily and at low cost.

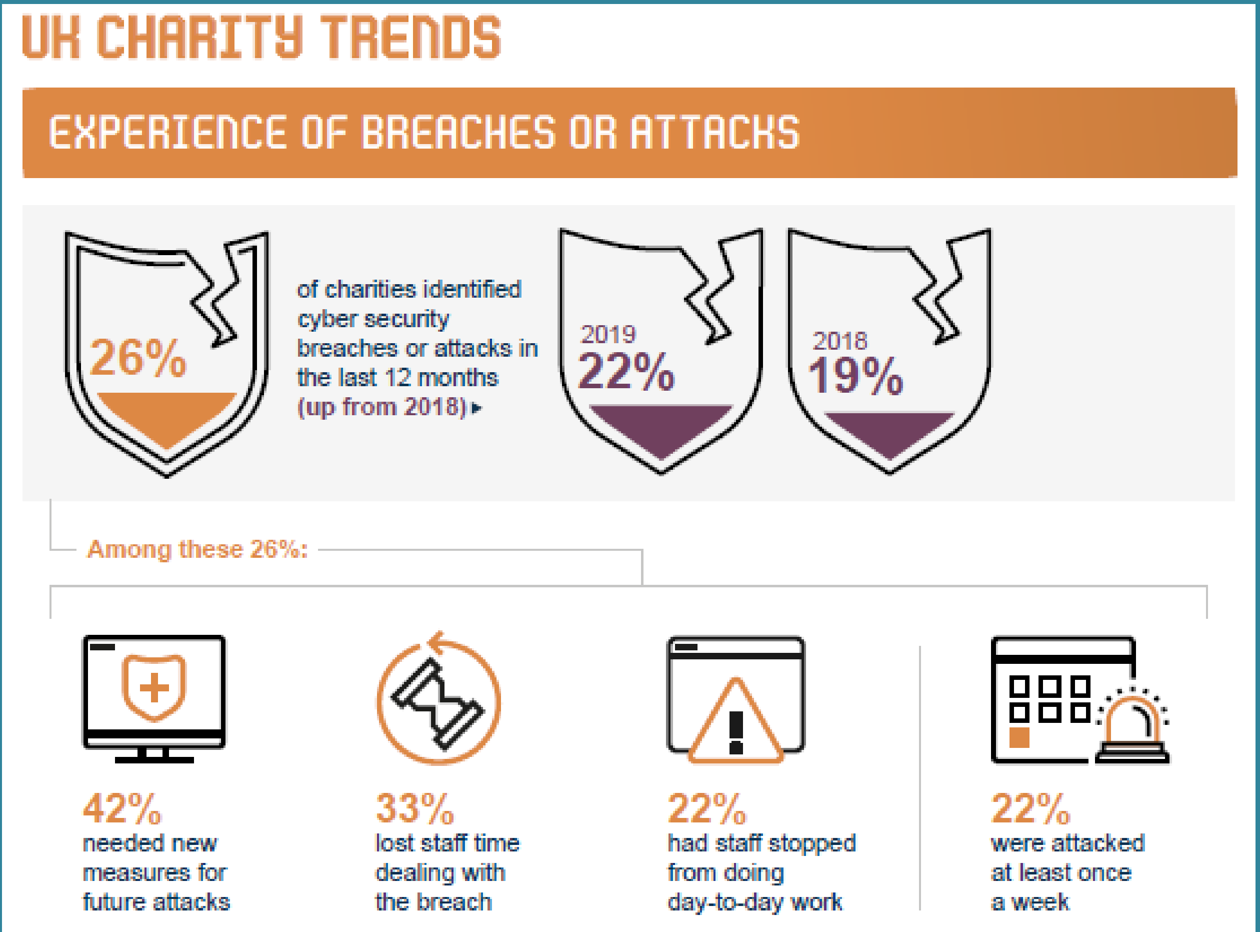
Cyber Aware

Stay connected.
Stay Cyber Aware.

Stay Safe Online – Top Tips for Staff

Top Tips for Staff training

Statistics…



UK CHARITY TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

26% of charities identified cyber security breaches or attacks in the last 12 months (up from 2018) ▸

2019 22%

2018 19%

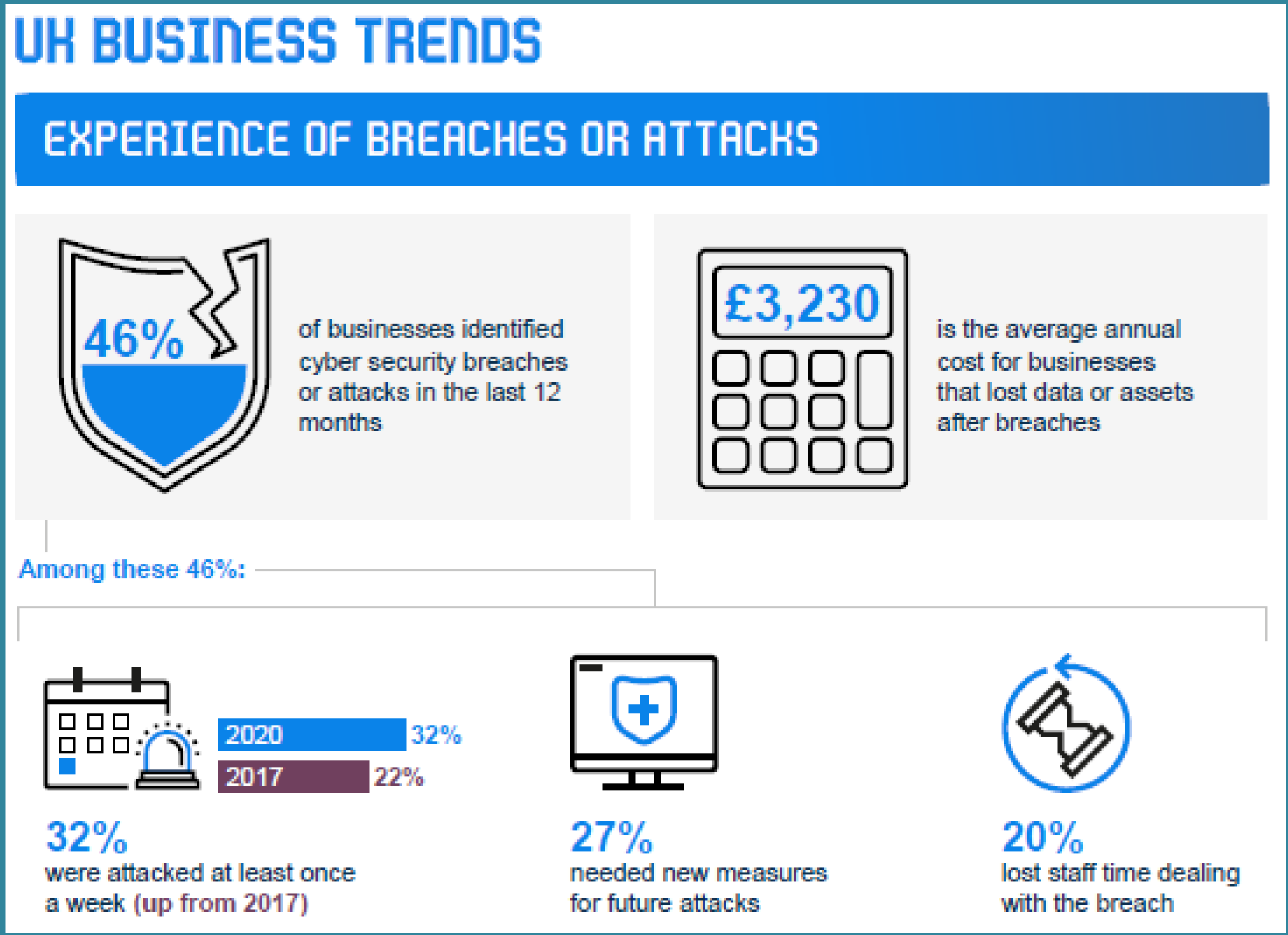
Among these 26%:

42% needed new measures for future attacks

33% lost staff time dealing with the breach

22% had staff stopped from doing day-to-day work

22% were attacked at least once a week



UK BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

46% of businesses identified cyber security breaches or attacks in the last 12 months

£3,230 is the average annual cost for businesses that lost data or assets after breaches

Among these 46%:

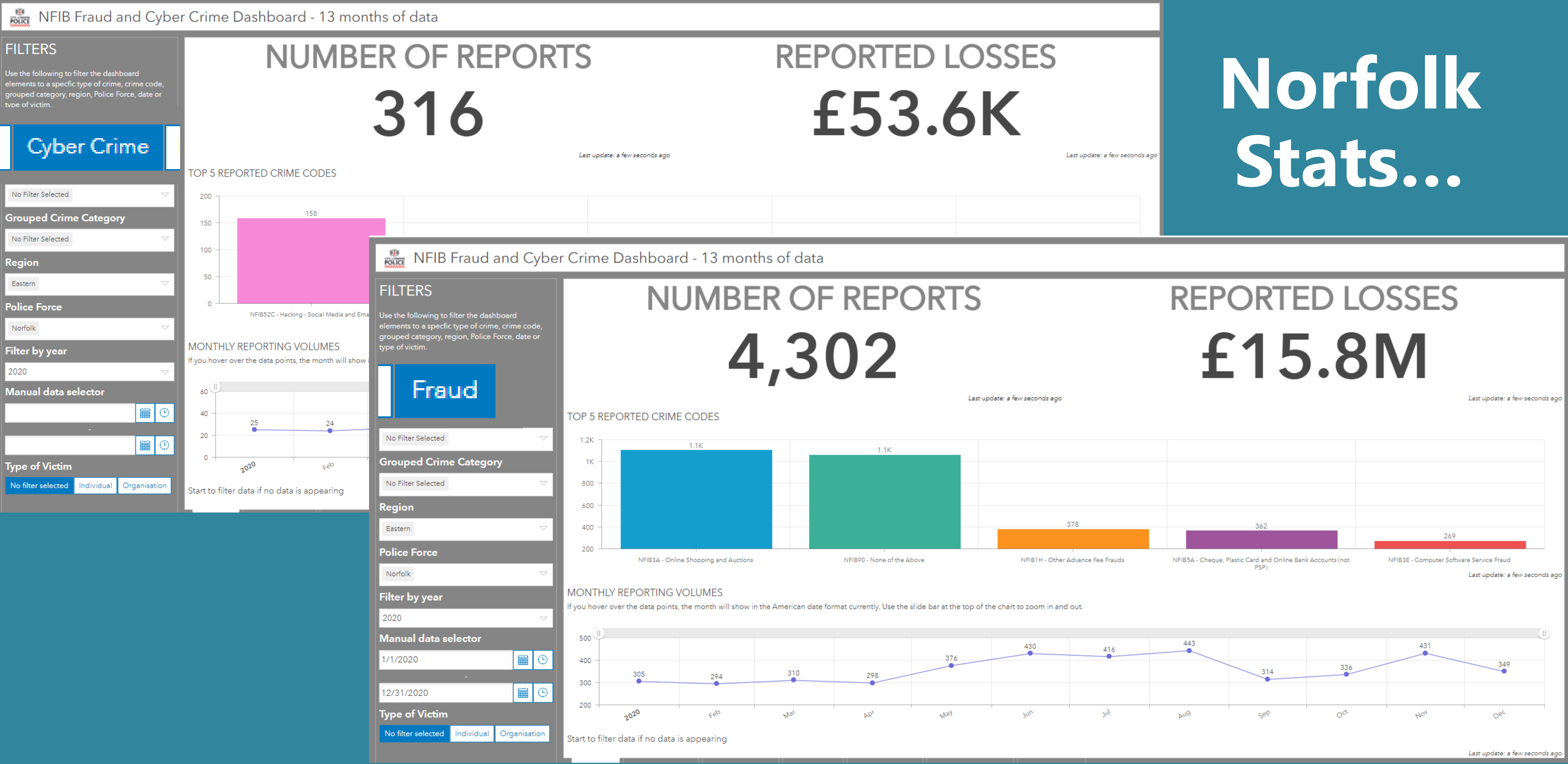
2020	32%
2017	22%

32% were attacked at least once a week (up from 2017)

27% needed new measures for future attacks

20% lost staff time dealing with the breach

Norfolk Stats…



NFIB Fraud and Cyber Crime Dashboard - 13 months of data

FILTERS

Use the following to filter the dashboard elements to a specfic type of crime, crime code, grouped category, region, Police Force, date or type of victim.

Cyber Crime

No Filter Selected

Grouped Crime Category: No Filter Selected

Region: Eastern

Police Force: Norfolk

Filter by year: 2020

Manual data selector

Type of Victim: No filter selected | Individual | Organisation

NUMBER OF REPORTS

316

Last update: a few seconds ago

REPORTED LOSSES

£53.6K

Last update: a few seconds ago

TOP 5 REPORTED CRIME CODES

MONTHLY REPORTING VOLUMES

If you hover over the data points, the month will show i

Start to filter data if no data is appearing

NFIB Fraud and Cyber Crime Dashboard - 13 months of data

FILTERS

Use the following to filter the dashboard elements to a specfic type of crime, crime code, grouped category, region, Police Force, date or type of victim.

Fraud

No Filter Selected

Grouped Crime Category: No Filter Selected

Region: Eastern

Police Force: Norfolk

Filter by year: 2020

Manual data selector: 1/1/2020 - 12/31/2020

Type of Victim: No filter selected | Individual | Organisation

NUMBER OF REPORTS

4,302

Last update: a few seconds ago

REPORTED LOSSES

£15.8M

Last update: a few seconds ago

TOP 5 REPORTED CRIME CODES

1.2K
1K
800
600
400
200
1.1K
NFIB3A - Online Shopping and Auctions
1.1K
NFIB90 - None of the Above
378
NFIB1H - Other Advance Fee Frauds
362
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)
269
NFIB3E - Computer Software Service Fraud

Last update: a few seconds ago

MONTHLY REPORTING VOLUMES

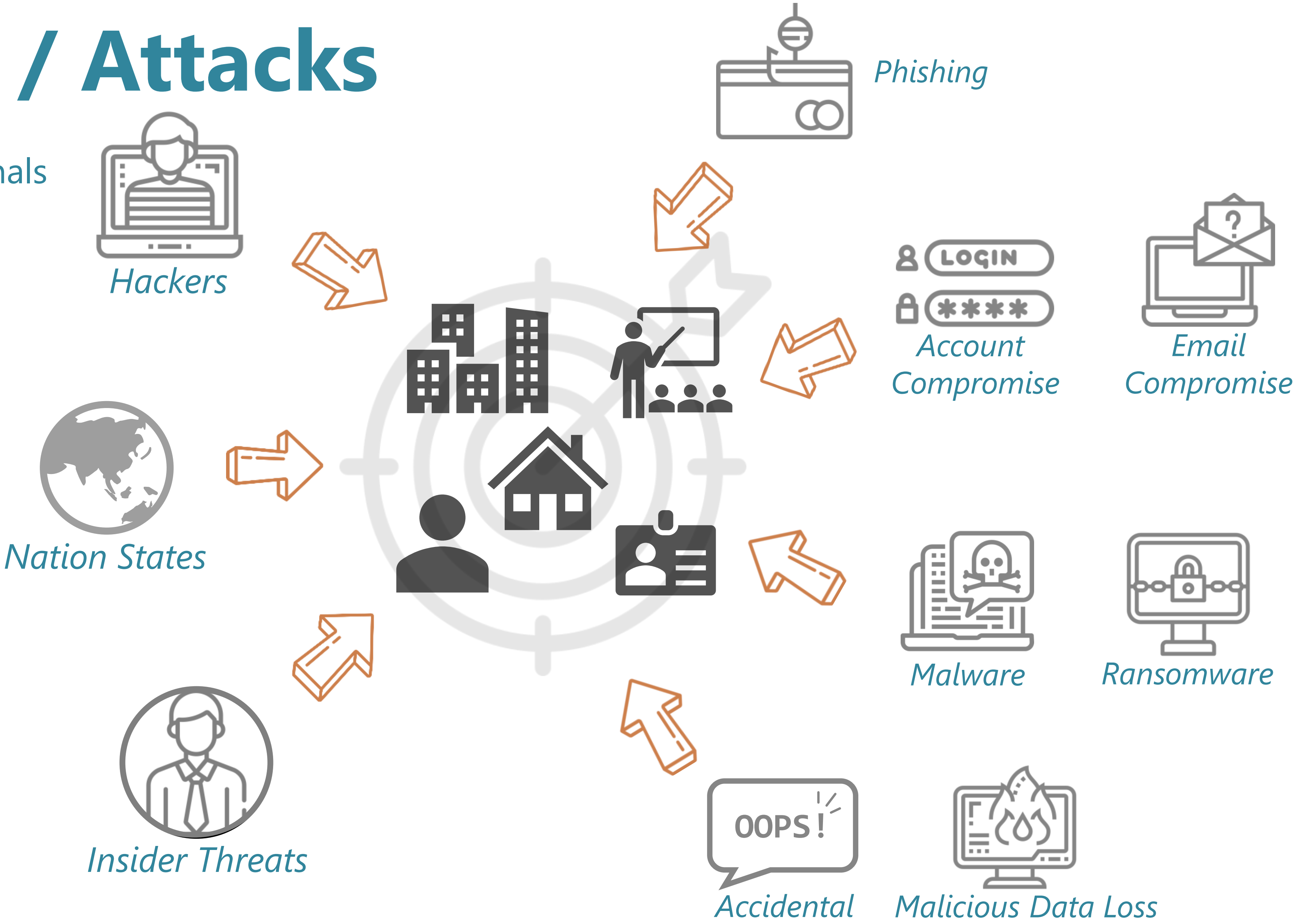
If you hover over the data points, the month will show in the American date format currently. Use the slide bar at the top of the chart to zoom in and out.

Start to filter data if no data is appearing

Last update: a few seconds ago

Attackers / Attacks

- Cyber Criminals
- Hacktivists
- Terrorists



Hackers

Nation States

Insider Threats

Phishing

Account Compromise

Email Compromise

Malware

Ransomware

Accidental

Malicious Data Loss

- Phishing
- Account /email compromise
- Malware - ransomware
- Insider threats

Social engineering

Phishing is the main cause of breaches - 45% of all the reports to the ICO.(ICO, 2019)

- Attackers attempt to trick users into doing 'the wrong thing'

Phishing

SMShing

Vishing

Phishing - general

- Disguise themselves as a trustworthy entity
- Aim is to make the user click a bad link or give away sensitive information

- *Could contain legitimate links*
- *Image of text to trick filters*
- *Sense of urgency / threats*
- *Link to cloud documents*
- *Numbers can be spoofed*
- *Email addresses / web domains with typos are used*
- *Fake sites are used to harvest details*

Have you received a phishing email to your email account this year?

In April (2020) Google (1.5 billion users) blocked 100 million phishing emails per day, a fifth of which related to COVID-19. *(BBC)*

Whaling

- Targets high-level decision makers

Spear phishing

- Personalised to their targets

Phishing

- Emails sent en masse

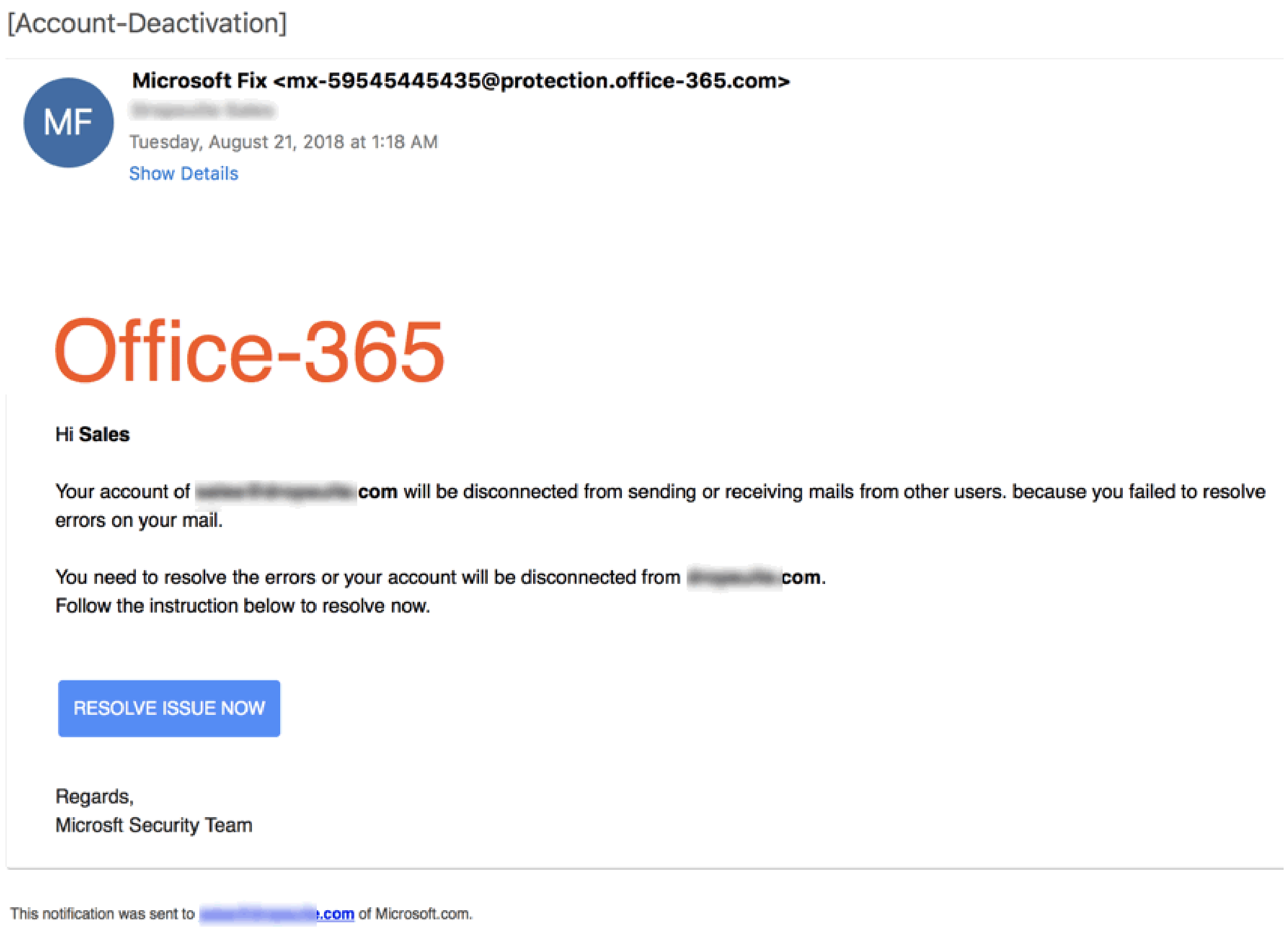
Could be from:

- *compromised internal account*

Potentially followed up with call

Targeted
Research Required
Personalised so more believable

Reel or Phish..



[Account-Deactivation]

Microsoft Fix <mx-59545445435@protection.office-365.com>
[redacted]
Tuesday, August 21, 2018 at 1:18 AM
Show Details

Office-365

Hi **Sales**

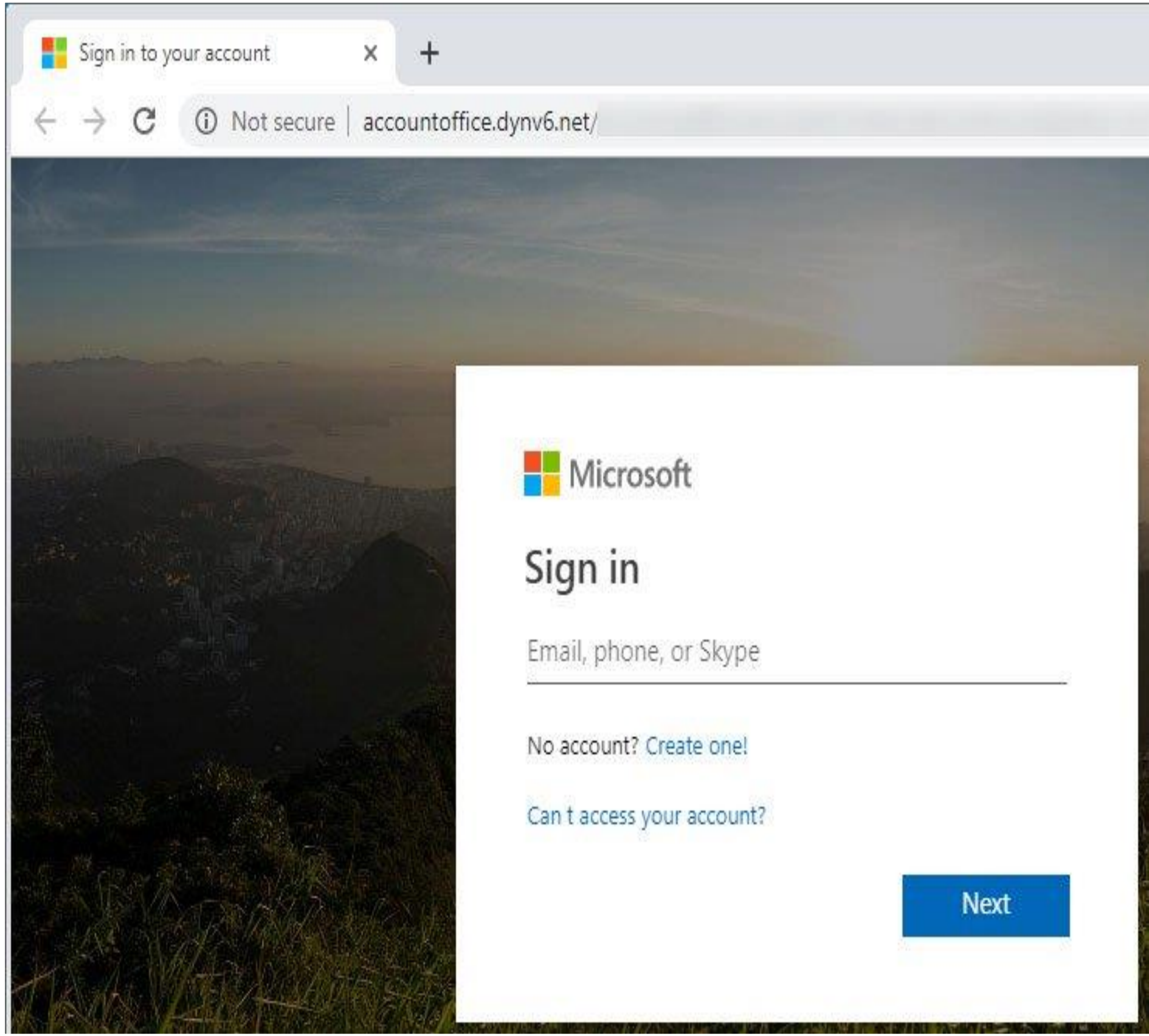
Your account of [redacted]**com** will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from [redacted]**com**.
Follow the instruction below to resolve now.

RESOLVE ISSUE NOW

Regards,
Micrösft Security Team

This notification was sent to [redacted].com of Microsoft.com.



Sign in to your account

Not secure | accountoffice.dynv6.net/[redacted]

Microsoft

Sign in

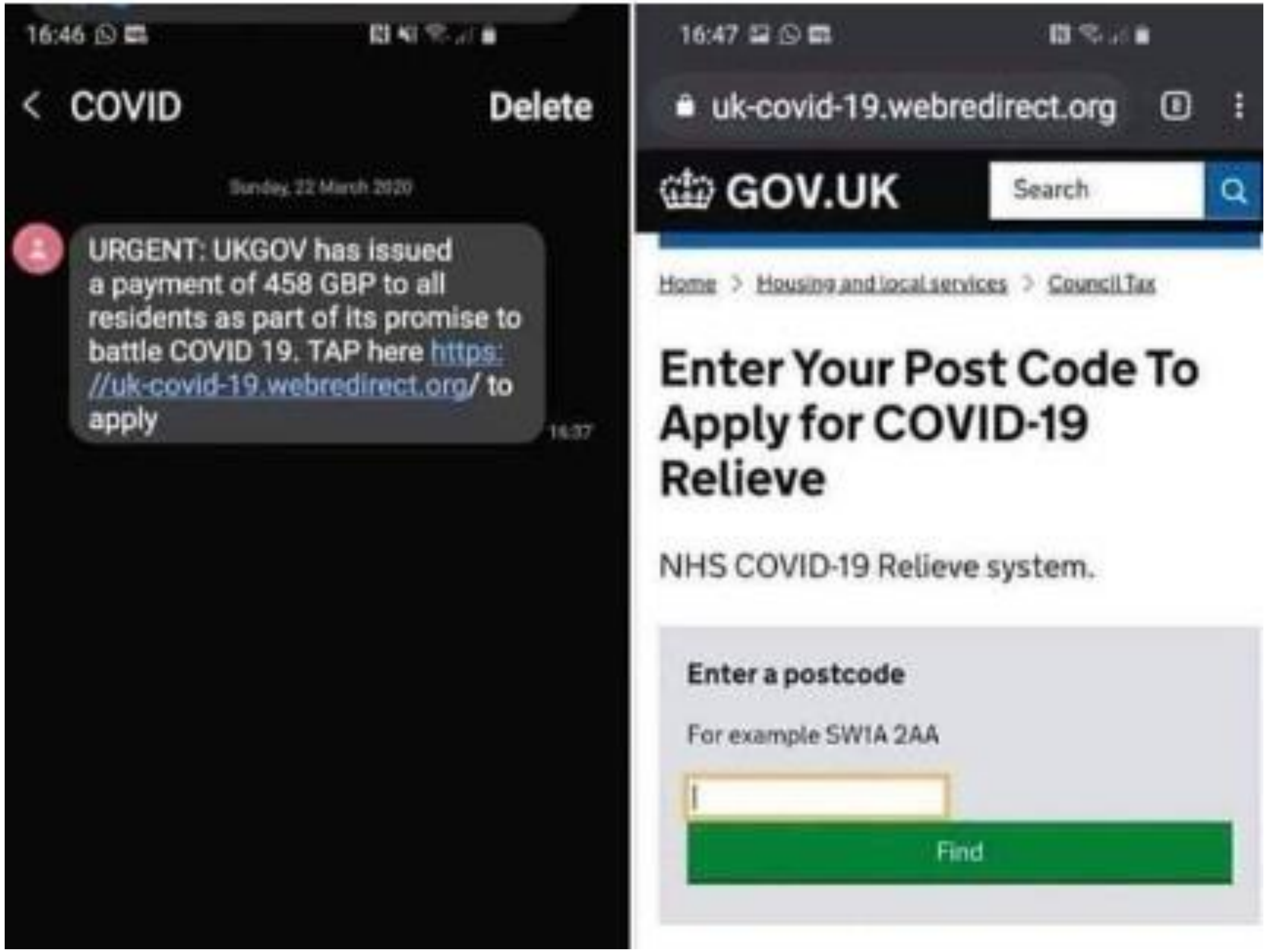
Email, phone, or Skype

No account? Create one!

Can t access your account?

Next

Reel or Phish..



16:46

< COVID Delete

Sunday, 22 March 2020

URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19.webredirect.org/ to apply

16:37

16:47

uk-covid-19.webredirect.org

GOV.UK Search

Home > Housing and local services > Council Tax

Enter Your Post Code To Apply for COVID-19 Relieve

NHS COVID-19 Relieve system.

Enter a postcode

For example SW1A 2AA

Find

Phishing – Tips for users

- Validate the other parties authenticity
- Check email addresses
- Hover over links to check where they go
- Visit sites via known URL’s

As of 31st January 2021 the number of reports received stand at more than 4,500,000 with the removal of more than 30,000 scams and 55,000 URLs.

- *Forward to the Suspicious Email Reporting Service – report@phishing.gov.uk*
- *Text messages can be reported by forwarding to 7726*

Do you / your organisation reuse passwords?

superman

password1

abc123

football

111111

monkey

qwerty1234

123456

password

qwerty

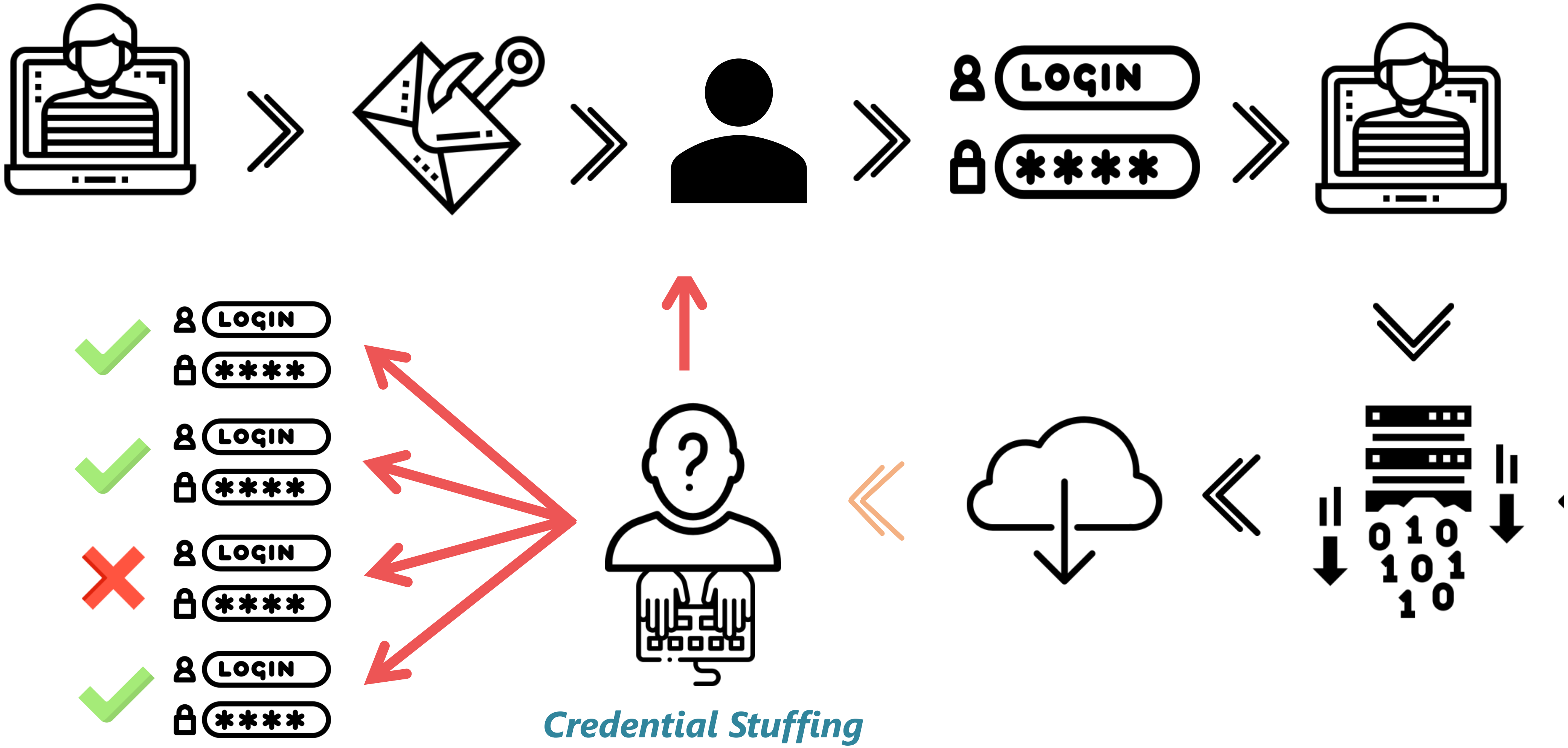
liverpool

qwerty123

1q2w3e4r5t

Account compromise example

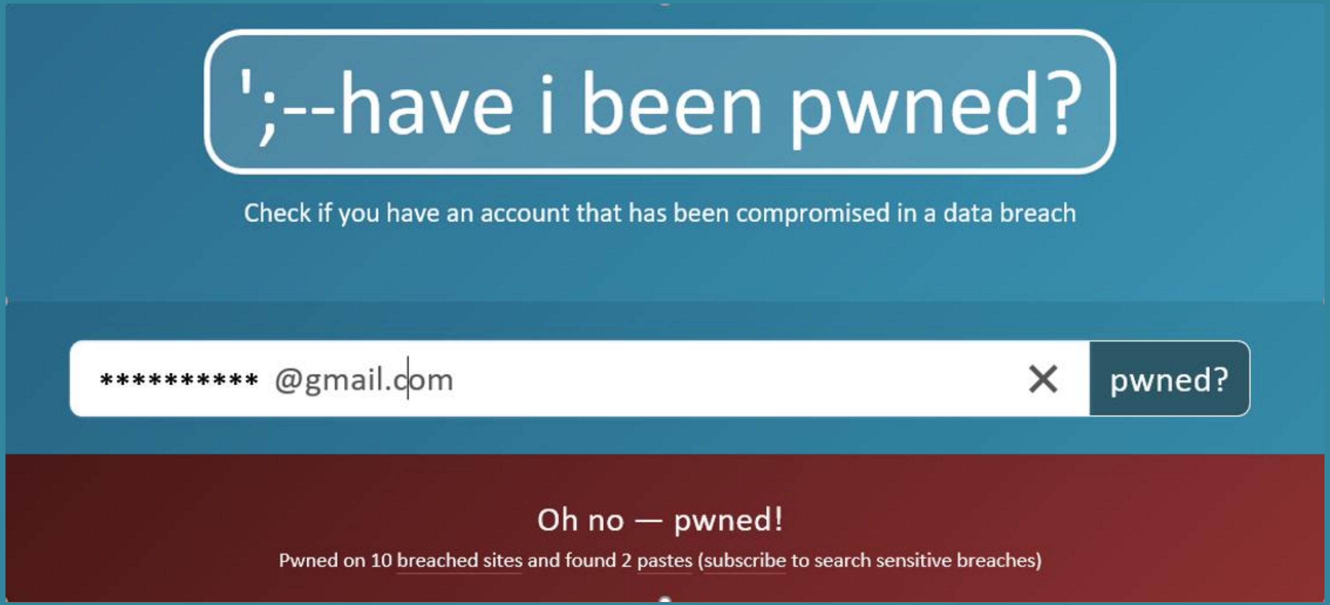
';--have i been pwned?



Credential Stuffing

Have your details ever been in a data breach?

You can check using www.haveibeenpwned.com



';--have i been pwned?

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

********** @gmail.com

Oh no — pwned!

Pwned on 10 breached sites and found 2 pastes (subscribe to search sensitive breaches)

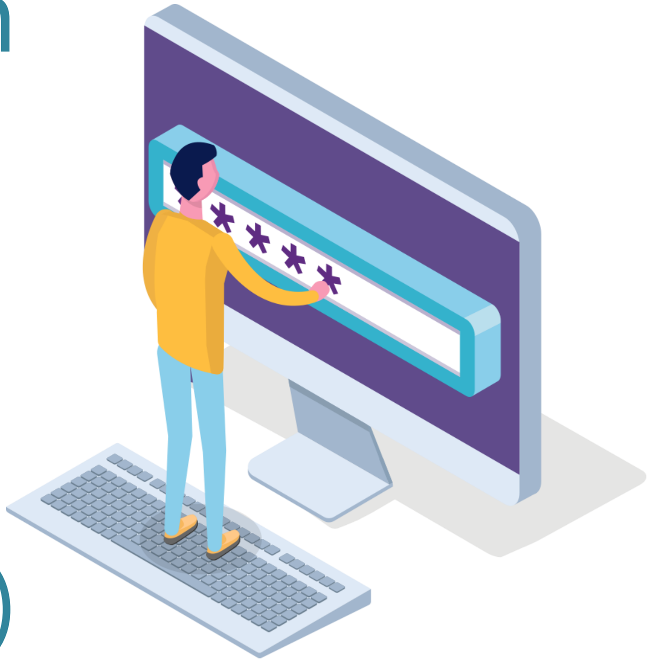
65% of people reuse passwords across multiple sites.

(Google 2019)

Top Tips

PROTECT YOUR EMAIL

- Use strong, separate passwords
  - ✓THREE RANDOM WORDS - Then add complexity, numbers and special characters
- Use a password manager / save passwords in browser
- Use two-factor authentication (2FA)



2 Factor Authentication (aka multi-factor, 2FA)

PASSWORD

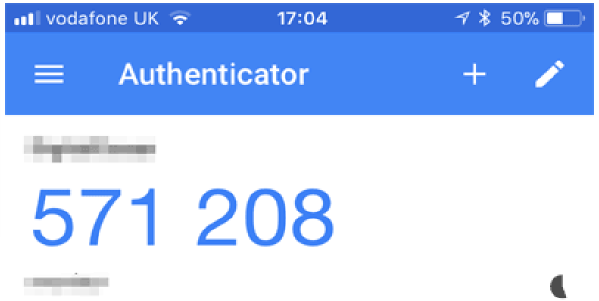
2FA

ACCOUNT ACCESS

Something you know

*TreeChairFish67^*

Something you have


vodafone UK 17:04 50%

Authenticator

571 208

If both correct then access granted

Cash Point example

****

Do your use 2FA for your email?

13% of people use the same password for all their accounts. (Google 2019)

Malware - Malicious Software

- Software intentionally designed to cause damage to a device / system
- There are many different types of malware

Can be triggered by opening a file, email link or opening an attachment

Ransomware

Aim: *Financial gain*

Target: *Organisations/anyone*

- Locks files – targets file extensions
- Can move across networks, connections and via Wi-Fi
- Can sit dormant to ensure backups are compromised
- Data can be extracted from network prior to attack
- Requires payment to gain unlock key

Do you backup important data regularly?

Ransomware attacks in the UK increased by 80% in between August and October 2020. (ITPro, Oct 2020)

Ransomware Actions

- Make regular robust backups
- Prevent malware from getting on to your device
- Prevent malware from running on devices
- *Disconnect any infected device from the network straight away*
- *Prepare for an incident*

Within your organisation do people only have limited access to data?

Human error caused 90% of cyber data breaches in 2019 (CybSafe/ICO)

Inside Threats

Staff are an organisations biggest strength and greatest weakness

- Negligent
- Malicious
- Compromised

Inside Threats Actions

- Training & awareness
- Encourage people to report anything suspicious.
- No blame culture - to encourage reporting of accidental actions
- Limited access to data
- Use 2 factor authentication

More Top Tips

- Update your devices
- Use anti-virus software

} *(set to auto update)*

- Backup your most important data

Phone ☎ | Mobile | Internet | Letter Box | Doorstep

Fraud

- COVID (vaccine, fines, payments)
- Investment Scams
- Romance Scams
- Courier Fraud
- TV Licencing
- Council Tax reduction
- Tech support scams

ARE YOU SCAM-SAVVY?

53% of people over 65 have been targeted by scams
Only 5% of scams are reported
(Friends Against Scams)

Friends Against SCAMS

FREE

NS Cyber as a resource

- Deliver Cyber Protect message & training
- Signpost and offer general cyber support and advice
- Lego Decisions and Disruptions roleplaying game to raise awareness of the importance of cyber security

🏭 Cyber Basics Review - in line with Cyber Essentials

🏭 Sponsors for CiSP – (Cyber Security Information Sharing Partnership) joint industry and government knowledge initiative

If you are a victim

Action Fraud 24/7
live cyber attacks

- Report to Action Fraud
- Keep copies of / photos of:
  - ✓ Logs (server / access / email)
  - ✓ Email headers
  - ✓ Any related documents
  - ✓ Keep forwarding rules

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

National Fraud
Intelligence Bureau

POLICE
NORFOLK & SUFFOLK
working together for you

National Cyber Security Centre
a part of GCHQ

ncsc.gov.uk

Cyber Aware

cyberaware.gov.uk

REPORT

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

ALSO FOR NEWS & ALERTS

Enable 2FA

Authy.org

';--have i been pwned?

haveibeenpwned.com

GET SAFE ONLINE .org

www.getsafeonline.org

TAKE FIVE TO STOP FRAUD™

takefive-stopfraud.org.uk

Friends Against SCAMS

friendsagainstscams.org.uk

citizens advice

age UK

POLICE & CRIME COMMISSIONER
NORFOLK

Norfolk
Against
Scams
Partnership

As a result of this presentation will you be reviewing your cyber security?

✉ **CyberProtect@Norfolk.police.uk**

@NSCyberCrime

www **norfolk.police.uk/advice/cybercrime**

smartsurvey.co.uk/s/Individual-NorfolkSuffolk2021