PROTECTING YOUR ORGANISATION AND YOURSELF FROM CYBERCRIME

John Greenwood - Cyber Security Advisor

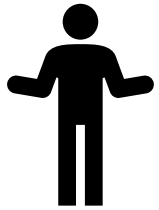
John.Greenwood@suffolk.police.uk

National Cyber Security Centre
a part of GCHQ

The single point of contact for individuals and organisations of all sizes in relation to cyber security.

90% of organisations have **not** sent staff on cyber security training

Cyber Security Skills Gaps Across UK Businesses In2021, DCMS



90% of cyber data breaches were caused by human error

Information Commissioners Office 2019

83% of organisations were the victim of Phishing

Cyber Security Breaches Survey 2021, DCMS

935% increase in double-extortion ransomware attacks since 2020

Weekly Threat report 03.12.2021, NCSC

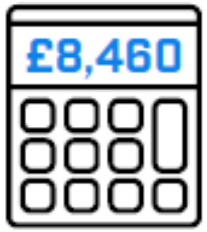
Cyber Security Breaches Survey 2021

Department for Digital, Culture, Media & Sport

UK BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

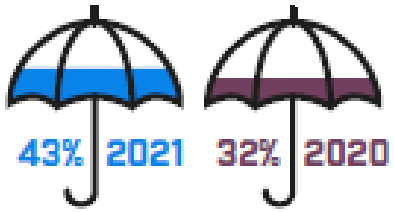
of businesses identified cyber security breaches or attacks in the last 12 months (down from 2020)



is the average annual cost for businesses that lost data or assets after breaches

£3,230 in 2020

43% have cyber insurance cover (up from 2020)



AMONG THE 39% IN 2021:

27% were attacked at least once a week

23% needed new measures to stop future attacks

*Cyber Security Breaches Survey 2021

Cyber Security Breaches Costs

Department for Digital, Culture, Media & Sport

	Short-Term Costs	Long-Term Costs
Direct Costs	• Cyber ransom and extortion costs • Financial theft • Staff response (overtime/contracting external staff)	• Loss of investors, donors or funding • Training costs (external resources) • Cyber security improvements
Indirect Costs	• Interruption of service • Lost, damaged or stolen outputs, data assets or property • Interruption of staffs' business as usual activities	• **Reputational damage** • Supply chain attrition • Loss of new and existing customers

"The costs in the aftermath of a cyber security incident tend to end up being much higher than the immediate direct costs faced by the organisation"

Cyber Breaches Survey 2021

*Analysis of the full costs of cyber security

- Social Engineering
- Digital Footprint
- Phishing
- Account Compromise / Business Email Compromise
- Ransomware

Social Engineering

Manipulation of people into performing actions or divulging confidential information.

"98% of cyber attacks rely on social engineering."

2021 Cyber Trends PurpleSec

"Criminals don't hack in, they log in."

Detective Inspector David Parkin (ret)

Be Aware of your Digital Footprint

- Avoid posting specific information about you, your organisation or role
- Check your privacy settings on social media
- Register for data breach notifications

https://haveibeenpwned.com

- What does your out of office auto-response say about you?
- Google yourself

Phishing - General

Messages from senders disguising themselves as a trustworthy entity

Aiming to make a recipient click a bad link, open an attachment and/or disclose sensitive information

- *Use images of text to trick filters*
- *Email addresses and web domains with typos are used*
- *Numbers can be spoofed*
- *Sense of urgency or threats*
- *Could contain legitimate links*
- *Links to fake websites which are used to harvest details*
- *Link to cloud documents*
- *Could come from a friend or colleague*

Anatomy of Phishing

Broad Attack Vector

Phishing

Messages sent / calls made en masse

High Quantity of Attacks

Messages/calls are broad and not personalised. Targets are often acquired from data which is in the public domain, previously leaked or stolen from elsewhere.

Targeted Attack Vector

Spear Phishing

Personalised to the target(s)

Whaling

Targeted at high-level decision makers

Research Required

Personalised to a specific target, so more believable

Additional Vectors:

- *Business E-Mail Compromise*
- *Potentially followed up with call*

Local Business Spear Phishing Example

Display name looked similar to their IT support address

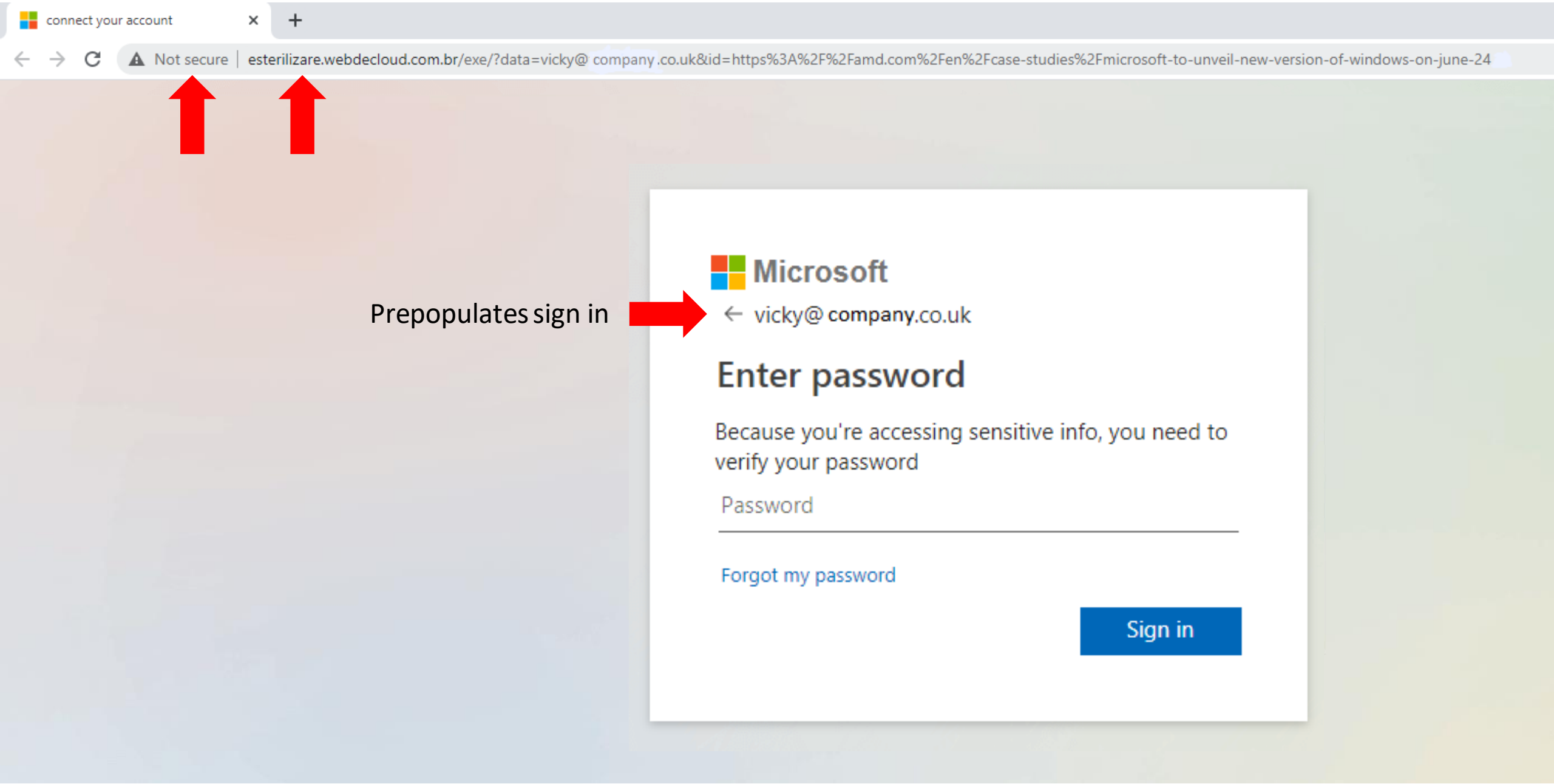
Sent to named financial controller

Company does use Office 365

Provided detail of a threat / worrying event. Fear of missing out.

Malicious Link

Company IT sign off


connect your account
Not secure
esterilizare.webdecloud.com.br/exe/?data=vicky@ company .co.uk&id=https%3A%2F%2Famd.com%2Fen%2Fcase-studies%2Fmicrosoft-to-unveil-new-version-of-windows-on-june-24
Prepopulates sign in
Microsoft
vicky@ company.co.uk
Enter password
Because you're accessing sensitive info, you need to verify your password
Password
Forgot my password
Sign in

Individual Phishing Defence

- Validate the sender's authenticity
  - Check email addresses
  - Hover over links to identify where they go (without clicking on them)
- Be proactive in your defence
  - Be mindful of what you share publicly (offline and online)
  - Always question why you're being asked to provide personal data
- Only visit genuine organisation websites or call genuine contact numbers

Organisational Phishing Defence

- Aim to make the organisation as difficult a target as possible
- Staff training
  - How to identify and report suspected phishing emails
- Filter or block incoming phishing emails
- Respond quickly to incidents
- Register alternative addresses

Suspect Phishing? Report It!

If you suspect an email is Phishing, help others by reporting it to:

report@phishing.gov.uk

Phishing text messages can be reported by forwarding them to:

7726

As of 31st October 2021 the number of reports received stand at more than **8,100,000** with the removal of more than **67,000** scams and **124,000** URLs.

Do you / your organisation reuse passwords?

Question:

Which of these passwords is the strongest?

1. qwerty123
2. Pa55w0rd
3. EpicCoffeeMonitor21@
4. %oe4D!3£

Cyber Aware

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)

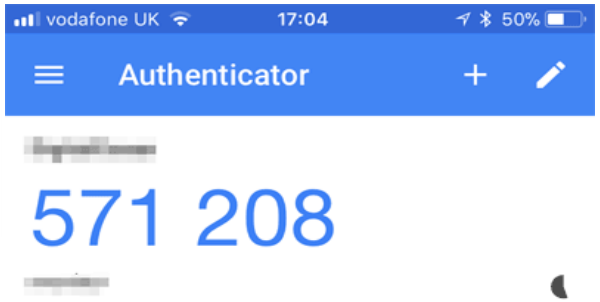
2 Factor Authentication (aka multi-factor, 2FA)

PASSWORD → 2FA → ACCOUNT ACCESS

Something you know

*TreeChairFish67^*

Something you have



If both correct then access granted

Cash Point example

****

Business E-Mail Compromise

- Often used in Spear Phishing and/or Whaling
  - Get you / your supplier to pay money into their account
  - Pretend to be someone internally
- Very convincing looking emails, often requesting payment
  - Changing regular payment details (Mandate Fraud)
  - Invoice interception and doctoring
  - Fake invoice scams
- Malicious Software Deployment

Defending The Organisation

- Establish with suppliers and internally, points of contact / procedures for handling and changing sensitive information
- Be willing to double check information via a different medium
- Check regularly for email forwarding rules
- Monitor / flag suspicious activity
- Use 2FA
- Be wary of oversharing company information

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

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

More Top Tips

Cyber Aware

- ☑ Update your devices
- ☑ Use anti-virus

} *(set to auto update)*

- ☑ Backup your most important data
  - Test these backups
    - *Can you recover from them in an emergency, how long would it take?*

Business Top Tips

- ☑ Limit physical access to computers and servers
- ☑ Restrict and enforce strict access to data and encrypt sensitive data
- ☑ Ensure you have relevant policies & procedures in place
- ☑ **Make your staff aware of cyber security threats and how to deal with them**

<u>If in doubt call it out!</u>

Cyber Insurance

National Cyber Security Centre
a part of GCHQ

- Has the organisation identified it's 'crown jewels' and assessed it's cyber risk?
- Does the organisation understand the cyber insurance policy?
  - What cyber security measures must be in place in order to claim against (or renew) it?
  - What does it cover (or not cover)?

What services and support are available to deal with a cyber incident?

How will it help the organisation get back on its feet, should something cyber-related go wrong?

If you are a victim

- Report to ActionFraud
- 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

Cyber Protect as a resource

FREE

- 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
  - A free assessment of your organisation's IT infrastructure in line with Cyber Essentials
- Sponsors for CiSP (Cyber Security Information Sharing Partnership)
  - A joint industry and government knowledge sharing initiative

- Free membership
- Aims to protect organisations in the East of England against cyber crime.
- Provide affordable testing and training services
- *Find out more at:* ***https://www.ecrcentre.co.uk***

THE CYBER RESILIENCE CENTRE FOR THE EAST

- Free tool to help members understand and monitor malicious cyber activity
- Monitoring and vulnerability scanning
- *Find out more at:* ***https://cyberalarm.police.uk***

POLICE CYBERALARM

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

TAKE FIVE TO STOP FRAUD™

takefive-stopfraud.org.uk

';--have i been pwned?

haveibeenpwned.com

GET SAFE ONLINE .org

www.getsafeonline.org

CYBER ESSENTIALS

cyberessentials.ncsc.gov.uk

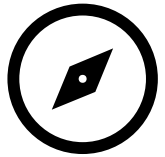
NO MORE RANSOM

nomoreransom.org

CiSP
Cyber-security Information Sharing Partnership

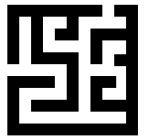
POLICE
NORFOLK & SUFFOLK
working together for you

NSCYBER



Cyber security is a **journey**, it should not be a one time consideration.

Cyber is a **business risk** and should be assessed and planned for as such.



Effective cyber security should **not sacrifice ease of use**.

Staff are a common exploited weakness, but with **regular training and awareness** they can provide an additional line of defence.

norfolk.police.uk/advice/cybercrime

CyberProtect@Norfolk.police.uk

@NSCyberCrime

NS Cyber

NSCyber.com/BusinessFeedback