inTEC BUSINESS

HACKED!

WELCOME: OUR WEBINAR WILL COMMENCE SHORTLY

THIS WEBINAR IS BEING RECORDED

inTEC BUSINESS

Welcome

OWEN COLLAR:

Head of Cyber Security Audit
& Lead Assessor of the Cyber Essentials Scheme

CERTIFICATION BODY CYBER ESSENTIALS PLUS

CERTIFICATION BODY CYBER ESSENTIALS

CERTIFICATION BODY IASME GOVERNANCE

Gold Microsoft Partner

Microsoft

UKAS ISO 9001 QUALITY MANAGEMENT

inTEC

What is hacking?

Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorised access to personal or organisational data.

Example 1

From: Claire Smith [mailto:claire.smith@silverdesigns.email]
Sent: 10 January 2023 12:17
To: Brian Young
Subject: FWD: RE: Legal/Consultancy fee overdue

Dear Brian,

Please pay the below asap and let me know once done

Regards.

Claire Smith

This is an e-mail from Silver Designs Limited (Company No. 045465816). The contents of this e-mail are confidential. Silver Designs Limited does not accept responsibility for the accuracy or compl
and then delete this e-mail. This e-mail and/or any replies to it, and any attachments may be intercepted, copied or monitored by Silver Designs Limited for the purpose of monitoring or keeping r
The contents are not to be regarded as a contractual offer or acceptance. The sender is not authorised to bind Silver Designs Limited. The views expressed in this e-mail are those of the sender an

Social engineering

User awareness training

Example 1

From: Gareth Wilson <g.wilson@abclaw.co.uk>
Sent: Tuesday, January 10, 2023 11:09:20 AM
To: Claire Smith
Subject: RE: Legal/Consultancy fee overdue

Hi Claire,

Further to our telephone conversation earlier find below the bank details for payment. Please ensure this is paid today.

SORT CODE: 19-12-06

ACCOUNT NUMBER: 52036971

AMOUNT: £12.109.00

REF: SD-0167

Regards

Gareth

Associate

ABC LAW

Social engineering

User awareness training

Example 1

From: Claire Smith [mailto:claire.smith@silverdesigns.email]
Sent: 10 January 2023 12:17
To: Brian Young
Subject: FWD: RE: Legal/Consultancy fee overdue

Dear Brian,

Please pay the below asap and let me know once done

Regards.

Claire Smith

This is an e-mail from Silver Designs Limited (Company No. 045465816). The contents of this e-mail are confidential. Silver Designs Limited does not accept responsibility for the accuracy or compl
and then delete this e-mail. This e-mail and/or any replies to it, and any attachments may be intercepted, copied or monitored by Silver Designs Limited for the purpose of monitoring or keeping r
The contents are not to be regarded as a contractual offer or acceptance. The sender is not authorised to bind Silver Designs Limited. The views expressed in this e-mail are those of the sender an

Social engineering

User awareness training

What is whaling?

Whaling is a highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email.

Whaling is digitally enabled fraud through social engineering, designed to encourage victims to perform a secondary action, such as initiating a transfer of funds.

Social engineering

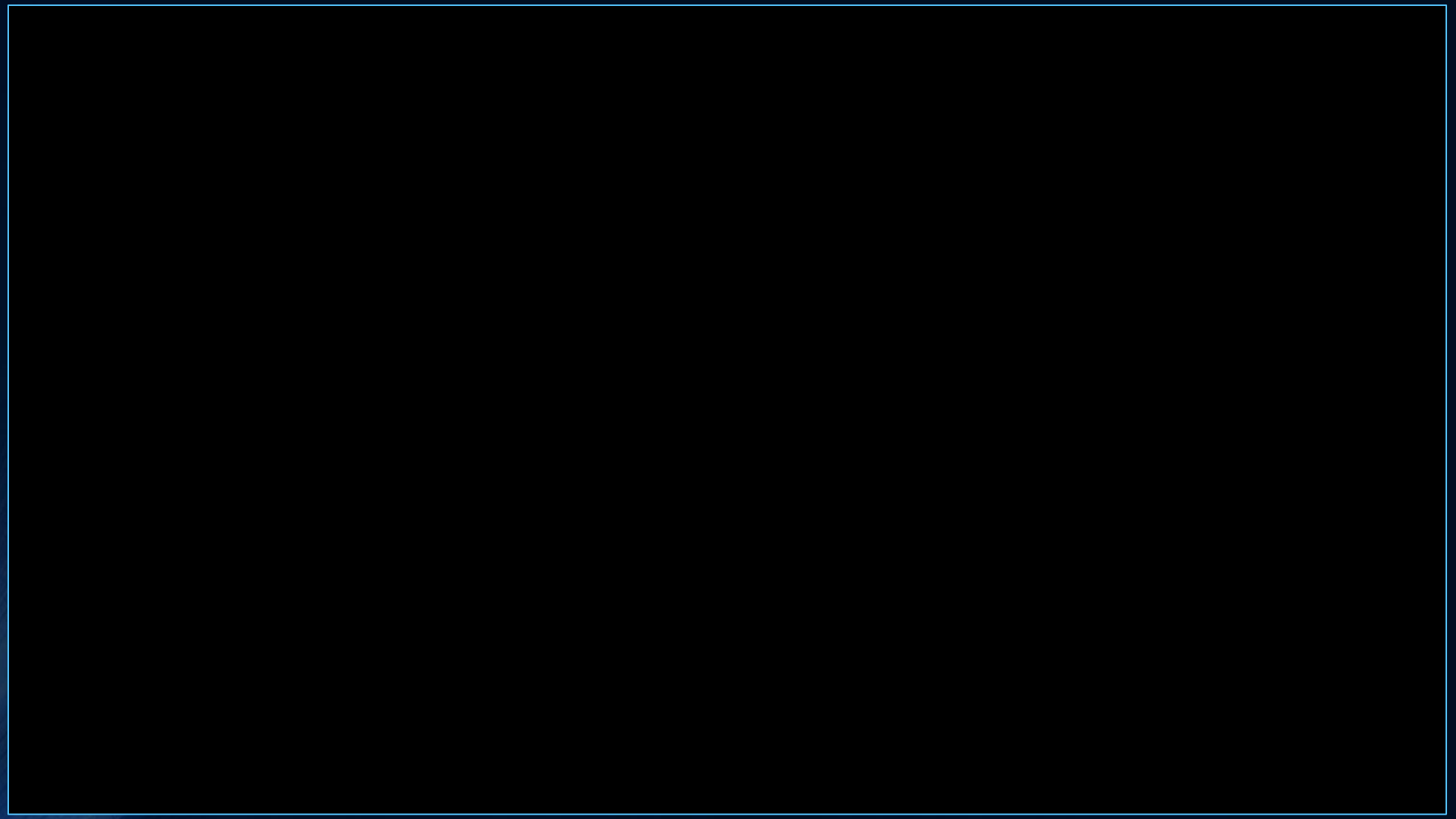
User awareness training

Lessons learnt

- Email filtering – imposter checking, use enterprise class mail filters
- User awareness training
- Check unusual transaction requests

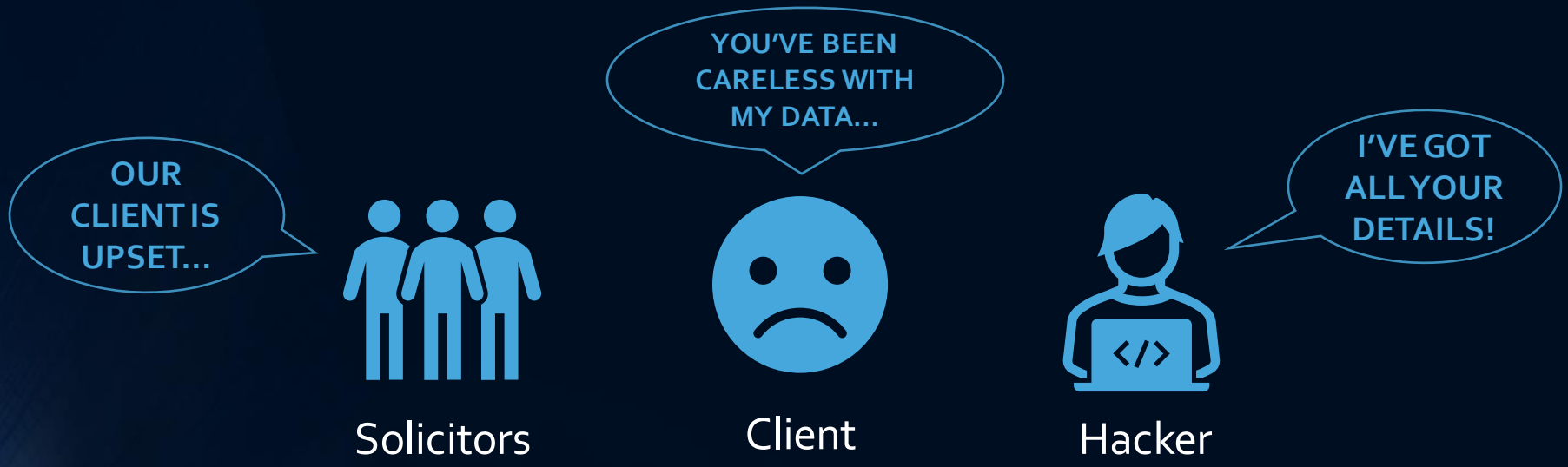
Social engineering

User awareness training



[Source: Proofpoint]

Example 2



Social engineering

Anti malware

User awareness training

Lessons learnt

- Fraudsters will do their homework and use open-source intelligence to gather information
- Anti-malware must be installed and up to date
- Don’t trust someone that rings you. Always ring back a trusted number
- Perform regular user awareness training

Social engineering

Anti malware

User awareness training

What is malware?

Malware is malicious software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.

Social engineering

Anti malware

User awareness training

Example 3

Backups Passwords

Lessons learnt

- Not all attacks are targeted
- Check your backups and have a plan
- Disable or delete old accounts
- Regular vulnerability scans
- Admission rules for MSP's or providers

Administrative access – what should you consider?

- Would a user account creation process help your organisation?
- Could you could create a set of rules around administrator accounts?
- Do you have a process for ensuring that employees do not use administrator accounts for day-to-day activities?

Social engineering

Anti malware

User awareness training

Example 4

Bring your own device policy

Lessons learnt

- Bring your own device policies
- Turn on two factor authentication
- No automatic logins
- Timed access, auto logout

Have you enabled MFA on all accounts?

- Additional protection
- Single use code via another device
- Single use code via authenticator app/token
- Additional considerations for businesses:
  - A managed/enterprise device
  - An app on a trusted device
  - A physically separate token
  - A known or trusted account

Social engineering

Anti malware

User awareness training

Example 5

Administrative use

User awareness training

Patching & updates

Managing user privileges

Backups

Lessons learnt

- Never use a computer as an administrator
- Always install Windows/Application updates
- File permissions
- Mail filtering
- Perform regular user awareness training
- Check your backups
- Cloud backups
- Consider Cyber Liability Insurance

Do you have a system for backing up your data?

- Cyber Essentials recommendation
- Your organisation is at risk of a cyber-attack, accidental damage or natural disaster
- Regular backups crucial

Social engineering

Anti malware

User awareness training

[Source: Jimmy Kimmel Live]

Summary – our top 10 tips

1. Administrative use

2. Social engineering

3. Bring your own device policy

4. User awareness training

5. Patching & updates

6. Anti malware

7. Unsupported operating systems

8. Passwords

9. Managing user privileges

10. Backups

Cyber Essentials 2023

- Clarification on firmware
- Third party devices
- Device unlocking
- Malware protection
- Guidance on zero trust architecture

inTEC BUSINESS

FREE Vulnerability Scan for your organisation...

CHAT: add your contact details via this webinar chat

EMAIL: owen.collar@intecbusiness.co.uk

CALL: 0345 565 1767

CERTIFICATION BODY CYBER ESSENTIALS PLUS

CERTIFICATION BODY CYBER ESSENTIALS

CERTIFICATION BODY IASME GOVERNANCE

Gold Microsoft Partner

Microsoft

UKAS ISO 9001 QUALITY MANAGEMENT

inTEC BUSINESS

Book your full Cyber Security Audit today...

CHAT: add your contact details via this webinar chat

EMAIL: owen.collar@intecbusiness.co.uk

CALL: 0345 565 1767

CYBER ESSENTIALS PLUS

CYBER ESSENTIALS

IASME GOVERNANCE

Gold Microsoft Partner

Microsoft

ISO 9001

Any questions?

Discover more at:

intecbusiness.co.uk/cyberaudit