Information Security

CODE OF CONDUCT

1. You're Running Late

Information security protects sensitive information from unauthorised activities.

The goal is to ensure the safety and privacy of important data such as customer account details, financial data, and intellectual property.

Cyber-attacks, the biggest information security threat organisations face, are increasing in frequency and complexity.

But more on that later, time to check your inbox before logging off for the day.

2. Password Expiration

Once you’ve read the email, select either the hyperlink or delete button to continue.

From: IT@InformationSecurity.co.uk

To: AlexDoe@email.com

Dear network user,

This email is to inform you that your company database pasword has expired.

Please follow the link below to update your password.

Passwordreset.co.uk/renewal

Sincerly,

IT Security Team

Option a: Click the link *(Hover text: I should probably sort this out before I leave.)*

Option b: Click 'Delete' *(Hover text: I’m not sure this is legitimate, I’ll delete it.)*

Correct option: Click 'Delete'

Feedback: This email is likely a phishing attempt, where criminals attempt to retrieve personal information such as passwords or credit card numbers by sending fraudulent messages.

Notice the spelling errors made in this email, password has one "s" and sincerely is missing an "e". Read your emails carefully!

3. Check the Invoice

Once you've read the email select either the attachment PDF or forward icon.

From: User8789@orange.co.uk

To: AlexDoe@email.com

Dear Supplier,

Please find attached outgoing payments 08715.

In case there is any discrepancy please inform us immediately.

Sincerely

Accounts Payable

This footnote confirms that this email has been scanned by the in-mail security system.

Option a: Click the attachment *(Hover text: This email looks legitimate, click on the attachment.)*

Option b: Forward to IT (*Hover text: Better to be safe than sorry, I'll check with IT.)*

Correct option: Forward to IT

Feedback: Don't mind the footnote, the sender's email address is generic and therefore suspicious. Never click on an attachment or hyperlink if you're unsure about its legitimacy. This email could contain malware, it's best to talk through next steps with your IT department.

4. Answer the DM

Your colleague has reached out to you with a question. Select the response you feel is most appropriate.

Message from John Colleague:

Hi, just a quick one.

One of our contractors has been in touch and informed us that they've had a security breach.

What do you think I should do?

Answer option a: Inform IT along with senior managers; as a third-party vendor their failings are our failings.

Answer option b: Nothing, it's their failure and doesn't affect us.

Correct option: A

Feedback: Often criminals will target third-party vendors in order to get to a larger more secure organisation. In this case damage control should be done and more senior people must be informed.

5. Appointment Reminder

Click the calendar icon if you feel the email is harmless and the delete button if you believe it's harmful.

From: DrSanjit@Myoptician.co.uk

To: AlexDoe@email.com

Dear patient,

This is a friendly reminder that you have an eye test tomorrow at 17:30 PM.

Please arrive at your appointment at least 15 minutes early and call ahead if for any reason you are no longer able to make it.

Kindest Regards,

Dr Sanjit and Team

Option a: Add to Calendar *(Hover text: This looks legitimate, add the reminder into your calendar)*

Option b: Delete *(Hover text: This looks suspicious, delete the email.)*

Correct option: Add to Calendar

Feedback: The email contains no suspicious contents, feel free to pop the appointment into your diary.

6. Hello from IT

From: IT@email.com

To: AlexDoe@email.com

Subject: Re:Fwd: Outgoing payments 08715

Good evening,

We've received the email you forwarded and reviewed its contents. We can confirm that this email contained a crypto virus known as "Ransomware". If you had clicked on the attachment, you would have been locked out of the system, with criminals demanding payment in exchange for renewed access.

As you know, information security is vital to ensuring the strength and growth of our organisation. Protecting the information of our clients and employees is our main priority. But we all have a part to play. With that in mind we wanted to provide you with a few tips on how best to protect your data.

- Make regular copies of your data and store it away from your main workspace.
- Use strong passwords.
- Monitor your emails closely and be wary of clicking attachments or links.
- Don't leave your laptop or paperwork unattended or in unsecure spaces.
- Lock your laptop when you're away from your workspace.
- Delete old documents and email from your device (remember to empty your recycle bin as well).

Sincerely,

The IT Department