

THE
CYBER
ESCAPE
ROOM
CO.

THE SECURITY EMAIL *PACK*



Five ready-to-edit emails for the
messages you send again and again.

From The Cyber Escape Room Co.

BEFORE YOU HIT *SEND*

Inbox - What's Inside

Cyber Security Awareness Month 01	Amy @ The Cyber Escape Room How to use this security email pack To: You
Phishing 02 Phishing gets harder to spot when the message looks normal, the timing...	Copy them. Change them. Make them sound like your organisation. > Swap everything in [BRACKETS] for your own details. > Change the examples to fit your teams. Finance, customer-facing and technical teams face different risks. > Use the language your organisation already uses. > Make the action specific: what to do, who to tell, how. Please don't swap the logo and send all five on Monday morning. Space them out, and connect them to something people can actually practice. Amy.
Password Security 03 People have heard "use a strong password" enough times. The more...	
Payment Requests 04 Payment fraud rarely looks like fraud. It looks like a supplier updating...	
Reporting Suspicious Activity 05 People sometimes hesitate because they aren't sure whether something...	

CYBER SECURITY AWARENESS MONTH

October gives security teams a useful excuse to get people talking about cyber security. That doesn't mean filling everybody's inbox with a month of reminders they stop reading by week two. Start by telling people what's happening, why it matters and how they can get involved.



Subject: Cyber Security Awareness Month starts here

Hi everyone,

October is Cyber Security Awareness Month.

Over the next few weeks, we'll be running [ACTIVITIES/SESSIONS/EXPERIENCES] to help everyone practice the security behaviours we rely on every day.

This isn't about catching people out or giving you another training module to complete. It's about getting better at the moments that actually matter. Spotting something suspicious. Challenging an unusual request. Knowing when to stop. Reporting something quickly when it doesn't feel right.

Here's what's coming up:

[ACTIVITY + DATE]
[ACTIVITY + DATE]
[ACTIVITY + DATE]

You can find the full schedule here: [LINK]

Get involved. Ask questions. Have a go.

And if you get something wrong during one of the activities? Good. Better here than during the real thing.

Thanks,
[NAME/SECURITY TEAM]

PHISHING AWARENESS

Phishing gets harder to spot when the message looks normal, the timing makes sense and the person asking appears to be somebody you trust. Use this one to remind people what deserves a second look and what to do when something feels off.



Subject: Before you click, take another look

Hi everyone,

Phishing emails are designed to make you act before you think.

They might look like a message from a colleague, supplier or senior leader. They might tell you something is urgent. They might ask you to open a document, follow a link, make a payment or hand over information.

Before you do anything, check:

- Does the sender address look right?
- Is the request unusual or unexpected?
- Are you being pushed to act quickly?
- Does the link go where you expect?
- Are you being asked for information or access you wouldn't normally provide?

If something feels wrong, stop.

Don't click the link, open the attachment or reply to the sender. Report the message using [INSERT REPORTING METHOD] or contact [SECURITY/IT TEAM].

You won't get in trouble for checking. A false alarm is much easier to deal with than a successful phish.

Thanks,
[NAME/SECURITY TEAM]

PASSWORD SECURITY

People have heard “use a strong password” enough times. The more useful message is what good account security actually looks like and what they need to do.



Subject: A quick check on your account security

Hi everyone,

A stolen password can give an attacker exactly what they need to get into an account.

A few simple habits make that considerably harder:

- Use a unique password for every work account
- Use [COMPANY-APPROVED PASSWORD MANAGER] where available
- Never share passwords with colleagues
- Turn on multi-factor authentication (MFA) where required
- Never approve an MFA request you didn't trigger yourself

If you get an unexpected login prompt or MFA request, don't approve it just to make the notification go away.

Stop and report it to [SECURITY/IT TEAM] using [REPORTING METHOD].

The same goes if you think a password may have been exposed. Tell us quickly so we can deal with it.

Thanks,
[NAME/SECURITY TEAM]

PAYMENT REQUEST

Payment fraud rarely looks like fraud. It looks like a supplier updating their details, or a senior leader who needs something paid today. Send this one to anyone who can make, approve or change a payment.



Subject: Before you pay, check it's real

Hi everyone,

Payment fraud doesn't usually look suspicious. It looks like a supplier changing their bank details, an invoice that's almost identical to the last one, or someone senior who needs a payment made before the end of the day.

And it isn't only email. A phone call or voice note can sound exactly like somebody you know.

Before you make or change a payment, check:

- Has a supplier asked to change their bank details?
- Is someone asking you to skip the usual approval process?
- Are you being told it's urgent, or to keep it quiet?
- Has the request come through an unusual channel?

If anything feels off, stop. Verify it using contact details you already hold, not the ones in the message. Call back on a number you know is genuine.

Nobody will be in trouble for delaying a payment to check it. We would much rather wait an hour than lose the money.

If something doesn't add up, report it to [SECURITY/IT TEAM] or [FINANCE CONTACT] using [REPORTING METHOD].

Thanks,
[NAME/SECURITY TEAM]

REPORTING SUSPICIOUS ACTIVITY

People sometimes hesitate because they aren't sure whether something is suspicious enough to report. That hesitation costs time. This one makes the expectation simple.



Subject: Something look wrong? Tell us.

Hi everyone,

You don't need to prove something is a cyber incident before you report it.

If an email looks strange, somebody makes an unusual request, you receive an unexpected login notification or something simply doesn't feel right, tell us.

Report it using [REPORTING BUTTON/EMAIL/PHONE NUMBER].

Include any useful details you have, but don't investigate it yourself. And report it as soon as you can.

If it turns out to be nothing, brilliant.

We would rather check ten harmless messages than miss the one that matters.

Thanks,
[NAME/SECURITY TEAM]

EMAILS *TELL* PEOPLE. PRACTICE *CHANGES* WHAT THEY DO.

Nobody learnt to handle pressure by reading an email about pressure.

The Cyber Escape Room Co. builds *immersive experiences* that put your people into the decision: cyber escape rooms, AI-powered phishing calls, digital missions and tabletop exercises.

Not another explanation of what they should do. A chance to find out what they actually do.

BOOK A CALL