Cumbria Fire & Rescue Service

Information Security Month October 2025

Newsletter 3 | Information Security – Take 5!

Welcome to the third of five newsletters which will be shared with you during October to mark Information Security Month.

Information Security Month is an international initiative aimed at raising awareness about cyber security threats and educating individuals and organisations on how to protect themselves.

The theme of this week's newsletter is Information Security – Take 5!

- What Phishing and Spear Phishing is
- How to spot and avoid a Phishing or Spear Phishing attack
- What to do if you've been caught out by a Phishing or Spear Phishing attack.

You'll also find some recent real life examples of Phishing attacks and the tell-tale signs that gave them away.

What is Phishing?

Phishing is a type of cybercrime where attackers impersonate trusted individuals or organisations such as government departments, IT support, or suppliers, to trick you into:

- Revealing sensitive information (e.g. passwords, bank details, or personal data)
- Clicking on malicious links that install malware or redirect to fake websites
- Opening harmful attachments that compromise CFRS systems.

Phishing is often sent by email but can also be sent by text, phone call and social media messaging.

What is spear phishing?

Spear phishing is a targeted type of social engineering attack. An attacker gleans information about an individual (e.g. from the internet and social media). This allows them to masquerade as a trusted source in an electronic communication. Messages may look genuine at first glance. This may lead the individual to click on links, accept software updates or open attachments. In doing so, the individual can unwittingly compromise sensitive information, provide access to organisational finances or facilitate technical attacks on company networks.

CFRS employees should be especially vigilant, as phishing attacks can target public sector systems to gain access to residents' data or sensitive CFRS information, disrupt services or commit fraud.

Slow down – think before you click to prevent a potential cyber security incident

Got a suspicious email?

1. Were you expecting it?
2. Do you know the sender?
3. Know the sender, but the message seems odd?
4. Does it urge you to click a link/attachment?
5. Is the content vague?
6. Does it use unusual grammar, tone, content, logos?

- ✓ Trust your instincts
- ✓ Hover, check
- ✓ Sense check links and the sender's address
- ✓ Roll your mouse pointer over the link to reveal its true destination. Is it completely wrong? Is it almost correct but with a spelling mistake or slight deviation?
- ✓ Roll your mouse pointer over the sender's email address to reveal their true address
- ✓ If something is odd, this is an additional red flag
- ✓ Verify before you trust. If something doesn't seem right, check with the sender using different pre-established contact details

If in doubt, check with **security@cumbriafire.gov.uk**.

CASE STUDY 1

Cumbria County Council HR

Cumbria County Council HR- Approved Y0 Memo - June Financial Execution REF =-BVNJ32

CC Cumbria County Council HR <brian@ ..com>
To

Cumbria County Council - Official_Docs_Guide_Digital_Capital_Approved_#83475483.pdf
118 KB

Hi, ,

Please review HR document.

Cumbria County Council HR Services.

Red Flags:

- The sender's real address has nothing to with Cumberland Council. "Cumbria County Council HR" shows in the sender's description, however the real address can be seen between <.....> If the email is read too quickly, there is a danger that you might miss this and focus on the description.
- The malicious actor has used the old name "Cumbria County Council".
- The content is vague.
- The email was unexpected.
- The email urges the recipient to click a link.

CASE STUDY 2

Emails from the Chief Executive of Westmorland & Furness and Cumberland Councils

Sam Plum

TR TIMELY RESPONSE NEEDED <quickjob45@gmail.com>
To
13:31

--
Hello ,

Real quick—what's the best number to reach you by message on WhatsApp either[personal or work number] ? I'll be reaching out soon and look out for my message on WhatsApp.

Many thanks.
Have a great day!

From: AUGUST, MONDAY 11TH <privattenewboxx230@gmail.com>
Sent: 11 August 2025 12:17
To:
Subject: Andrew Seekings

Hello ,

Wishing you a productive and successful day. Kindly take a moment to re-affirm your current cell number? I intend to contact you shortly via text or call.

Thank you.
Andrew Seekings

Red Flags:

- Mimicry and authority – the sender is purposing to be a trusted person of authority (in the above cases it is the Chief Executive of both Cumberland and Westmorland & Furness Council).
- The mention of WhatsApp or texts - this is often used to divert users to another platform where their messages are less likely to be tracked and spotted. The WhatsApp profile will pretend to be the trusted person in authority and will likely show their picture
- The email address is not the Chief Executive's council email address, it is a Gmail address. A trusted person of authority at Cumbria Fire & Rescue Service, such as the Chief Fire Officer, will never reach out from a personal email address.
- Vague content, usually asking for a "favour" or whether you shop on "Amazon". Further messages could ask you to buy vouchers, with an excuse as to why they cannot do it themselves or inventing an emergency. The Service will never ask you to do this.

There are no links or attachments here, but follow-up messages will likely request that you spend money (financial scam), divulge sensitive or personal information or click a link/attachment. It is best not to reply to these messages at all. Replying confirms to the sender that your email account is active and that you are likely to respond to future phishing attempts.

CASE STUDY 3

Email from Payroll

From: Payroll@westmorlandandfurness.com KYY8iYVrtUJUMx0eNrbYAhRPsluIgT68CtwnkG4jJecfxaL53om6GZaxlrFnMCCkosVTsvd2xheGM <hostmaster@guam.net>
Sent: 20 August 2025 01:20
To:
Subject: Reminder for Wednesday August 20, 2025 to-do list 8e623a57-412b-4423-9c17-eed7f6f0c69a

Hi,

Please find attached the updated for your reference.

Attachments:

- 1 PDF pages
- 1 Excel file (XLSX)

Document size: 148 KB

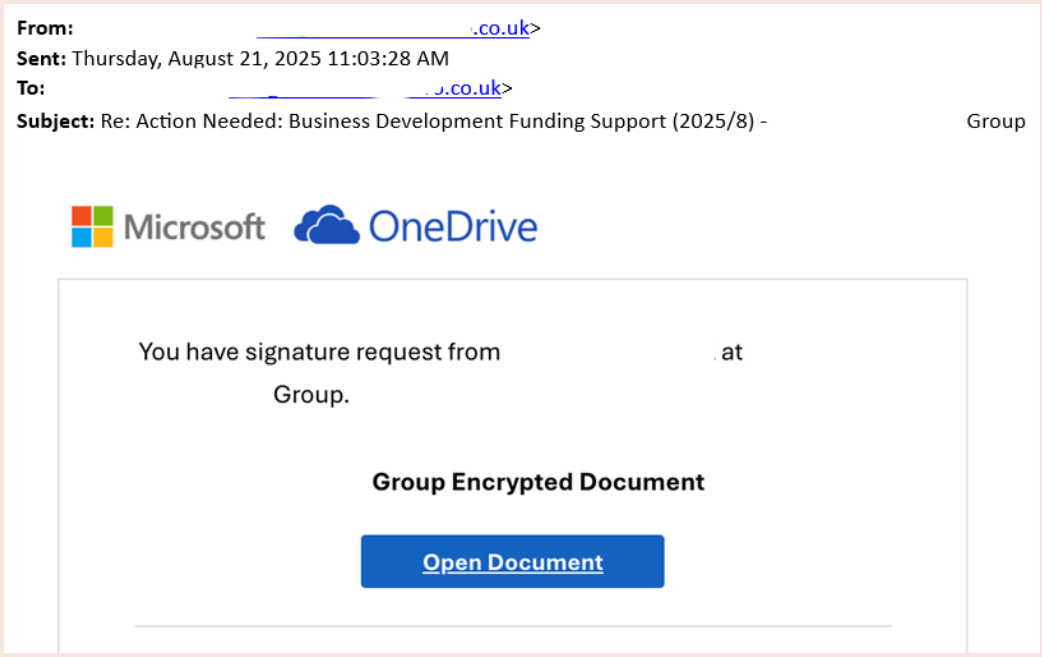
PDF Password: You should receive the password email shortly. If you don't receive it within [timeframe, e.g., "the next 30 minutes"], please check your spam folder.

Red Flags:

- An imitation council email address has been used in the sender description to trick the user who may not read the sender's actual address (an @guam.net address). Also notice the imitation is not a good one, as it ends in .com rather than .gov.uk.
- The email content is vague.
- The email contains unexpected links and attachments.

CASE STUDY 4

Malicious link in an email



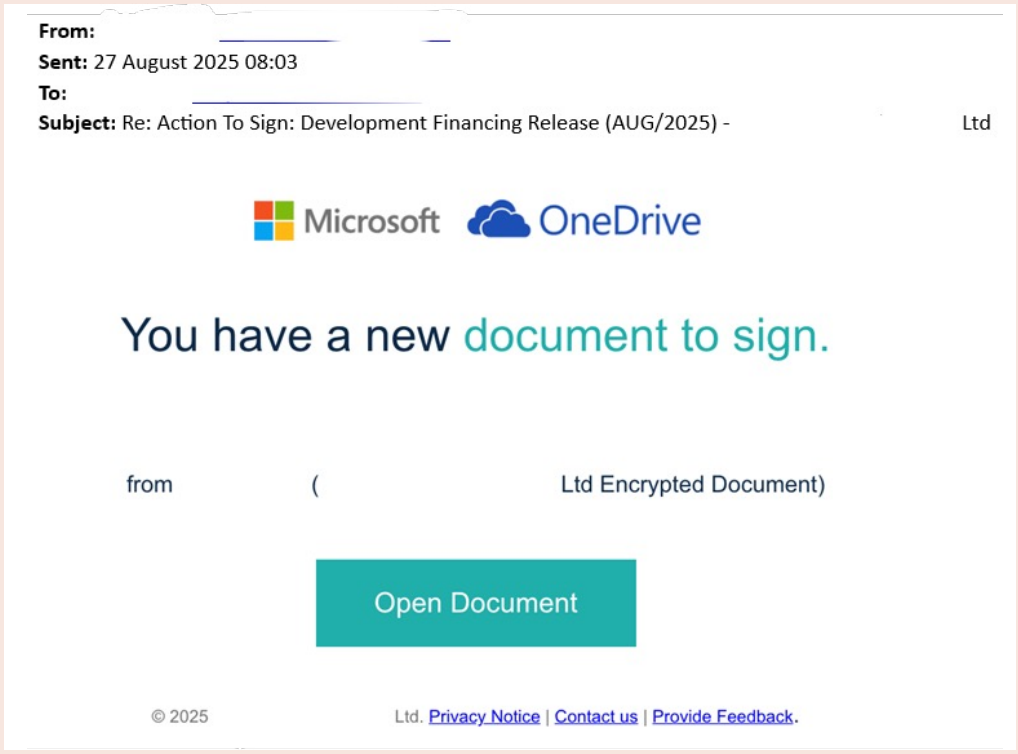
From: .co.uk>
Sent: Thursday, August 21, 2025 11:03:28 AM
To: .co.uk>
Subject: Re: Action Needed: Business Development Funding Support (2025/8) - Group

Microsoft OneDrive

You have signature request from at Group.

Group Encrypted Document

Open Document



From:
Sent: 27 August 2025 08:03
To:
Subject: Re: Action To Sign: Development Financing Release (AUG/2025) - Ltd

Microsoft OneDrive

You have a new document to sign.

from (Ltd Encrypted Document)

Open Document

© 2025 Ltd. Privacy Notice | Contact us | Provide Feedback.

Red Flags:

- Unexpected sharing of a document via OneDrive or SharePoint link. If the sender is known, always check with them via a different pre-established contact method (e.g. telephone), whether they have shared the link. It may be that their account has been compromised by a malicious actor – it's not really them emailing you!
- The sender has sent the email to themselves and bcc'd you in, and no doubt many other people, in the hope that someone will click the malicious link. The link could lead to a malicious website, document, ask for user name and password etc.

CASE STUDY 5
Remittance email

Remittance Copy and Certificate c884d3e0794a977ab4f5718025342732

AP Queries <alice@ .co.uk>(AP Queries via edendc.onmicrosoft.com)
To

Reply | Reply All | Forward

Fri 29/08/2025 09:52

We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.

Remittance Copy and Certificate c884d3e0794a977ab4f5718025342732
Outlook item

WARNING:

********WARNING: Who is this email really from - ? It may not be the person you think it is! Check from internal sources before responding! Don't be scammed!*********

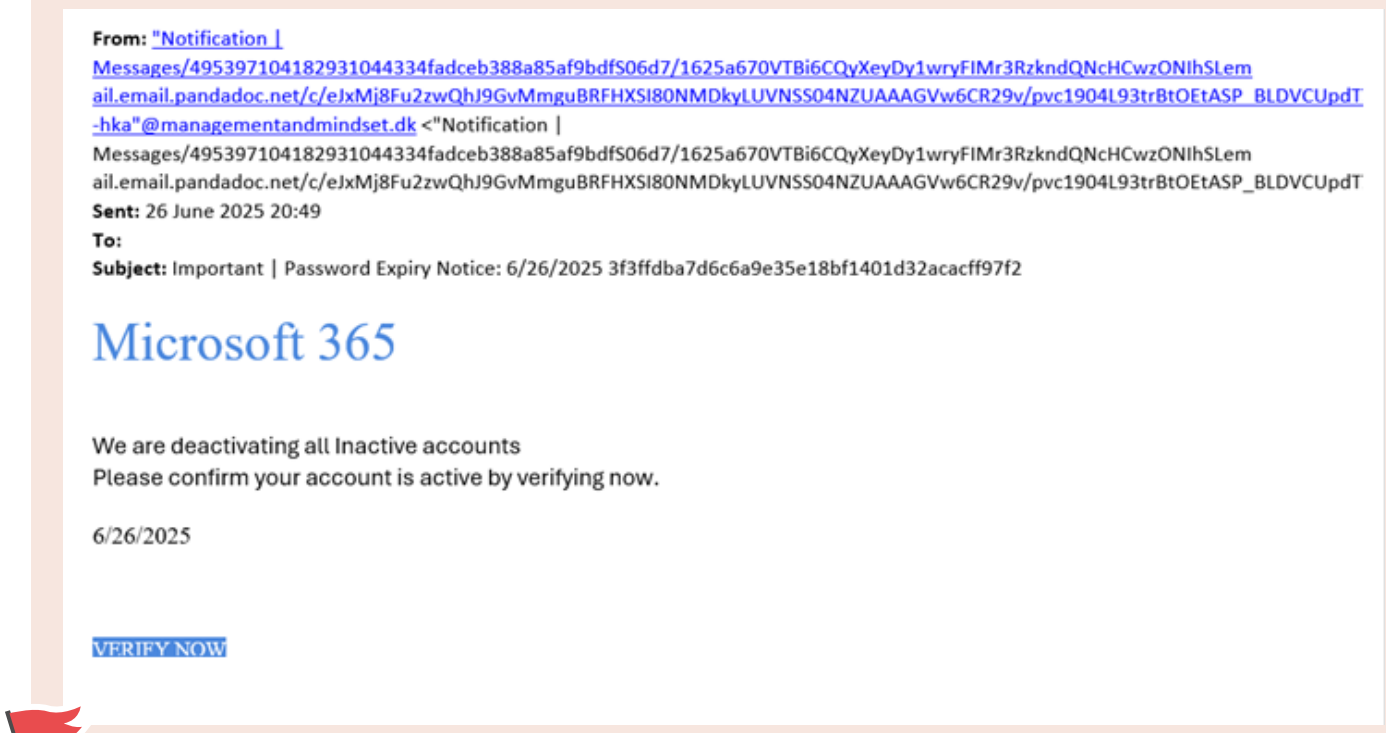
Email attachments may contain malicious and harmful software. If this email is unsolicited and contains an attachment DO NOT open the attachment and advise the ICT Service Desk immediately. Never open an attachment or click on a link within an email if you are not expecting it or it looks suspicious. Do not forward chain emails.

Red Flags:

- The email content is vague.
- The email contains an unexpected email attachment.
- The sender's actual address (between < and >) has nothing to do with the purported sender in the address description (Eden District Council).
- This email has likely been sent from a compromised account.

CASE STUDY 6

Fake Microsoft emails: Deactivating inactive accounts



From: "Notification | Messages/495397104182931044334fadceb388a85af9bdfS06d7/1625a670VTBi6CQyXeyDy1wryFIMr3RzkndQNcHCwzONIhSLem ail.email.pandadoc.net/c/eJxMj8Fu2zwQhJ9GvMmguBRFHXSI80NMDkyLUVNSS04NZUAAAGVw6CR29v/pvc1904L93trBtOEtASP_BLDVCUpdT -hka"@managementandmindset.dk <"Notification | Messages/495397104182931044334fadceb388a85af9bdfS06d7/1625a670VTBi6CQyXeyDy1wryFIMr3RzkndQNcHCwzONIhSLem ail.email.pandadoc.net/c/eJxMj8Fu2zwQhJ9GvMmguBRFHXSI80NMDkyLUVNSS04NZUAAAGVw6CR29v/pvc1904L93trBtOEtASP_BLDVCUpdT
Sent: 26 June 2025 20:49
To:
Subject: Important | Password Expiry Notice: 6/26/2025 3f3ffdba7d6c6a9e35e18bf1401d32acacff97f2

Microsoft 365

We are deactivating all Inactive accounts
Please confirm your account is active by verifying now.

6/26/2025

VERIFY NOW

Red Flags:

- CFRS will never ask you to change your password or verify your account via a link in an email.
- The sender's address is not a council address.
- Urgency.
- Poor logos.
- Hovering over the "Verify Now" link shows an unusual destination (to a Google address).

Remember

If you click on a link/attachment and afterwards doubt the legitimacy of the email, tell ICT / Information Security as soon as possible, especially if you have divulged your password.

No blame culture

Staff should not be afraid to tell us if they have made a mistake. Quick reporting is the key to remediate the situation effectively.

Report

Please report any particularly convincing phishing emails to Information Security at **security@cumbriafire.gov.uk**. Information Security may wish to check whether anyone else has received the email and warn others.

Unsure?

No one should feel silly for asking Information Security for a second opinion on whether an email looks suspicious. Spear Phishing can be very hard to spot!

Live Examples

Financial Scams

CFRS are witnessing an increase in scams.

Recent examples include elaborate social engineering of employees to defraud for financial gain.

Other examples have included the compromising of CFRS suppliers and partners' ICT solutions enabling the fraudsters to trick CFRS employees into believing they are representing an organisation when they are not.

Attempted frauds have included change of bank payment details.

When presented with an invoice or an email with bank payment details on you must double check with the organisation to validate.

This is equally important in work, but also in your personal life. Remember always authenticate bank payment details by contacting the organisation directly (not just by email), your email may have been compromised!

Always authenticate who you are communicating with.

Are they really the person they say they are?

As well as watching out for scams, you should remain vigilant when external requests come in for access to information. Does the request raise suspicions and is the person asking for the information legally entitled to it?

Remain vigilant.

Phishing emails – What can happen if you click?

CFRS continues to block phishing emails. However a small number do still get through.

A recent example convinced colleagues to click on a link that installed a keyboard logger onto the laptop.

All keyboard actions were then recorded and would have been sent to a malicious foreign website if ICT counter measures had not prevented this.

Remain vigilant when opening emails and clicking on links, especially at home, where you may not have counter measures in place to prevent such malicious activity.

Read the National Cyber Security Centre's online guide - **Phishing: Spot and report scam emails, texts, websites and calls**.

Send us your comments and feedback

Share your comments and feedback with us, including any suggestions for how information security could be improved, or an example of good Information Security practice from a colleague, or team.

The best examples will be included in our fifth and final newsletter at the end of the month.

Send your comments, suggestions and examples of good Information Security practice in an email with the subject line **"Information Security Month Feedback"** no later than Friday 24 October to **security@cumbria.fire.gov.uk** and remember to include your full name and contact details.

Thanks for reading this far! The theme of next week's newsletter will be Records Management

In the meantime, if you have any questions, please send them to: **security@cumbriafire.gov.uk**.

#StrongPasswords #CyberAware #BrowseSafe #ThinkCyber #MindfulClicks #OwnYourSecurity