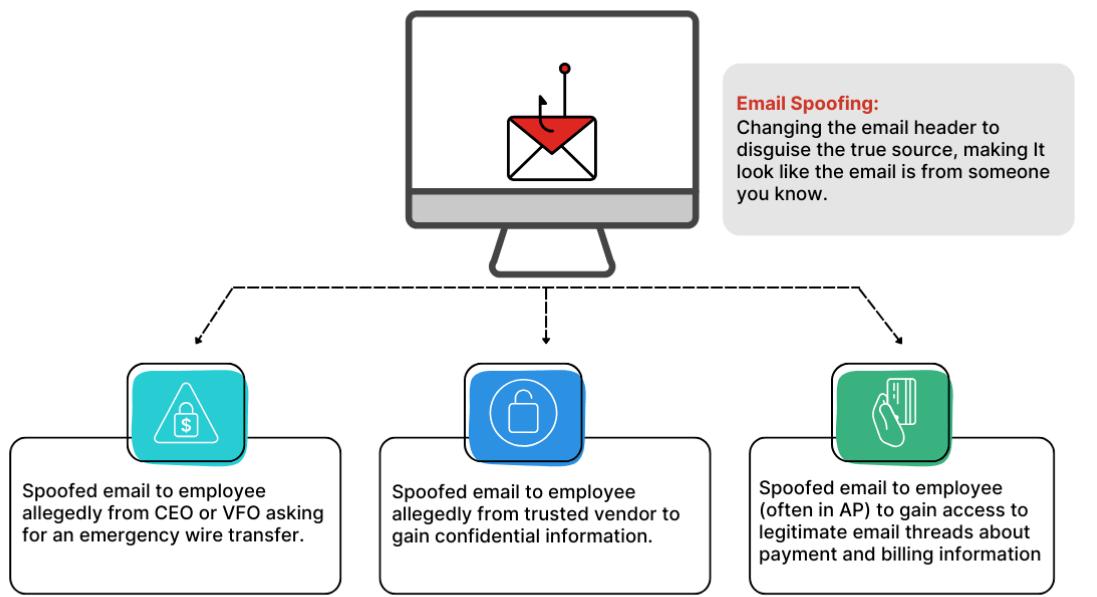


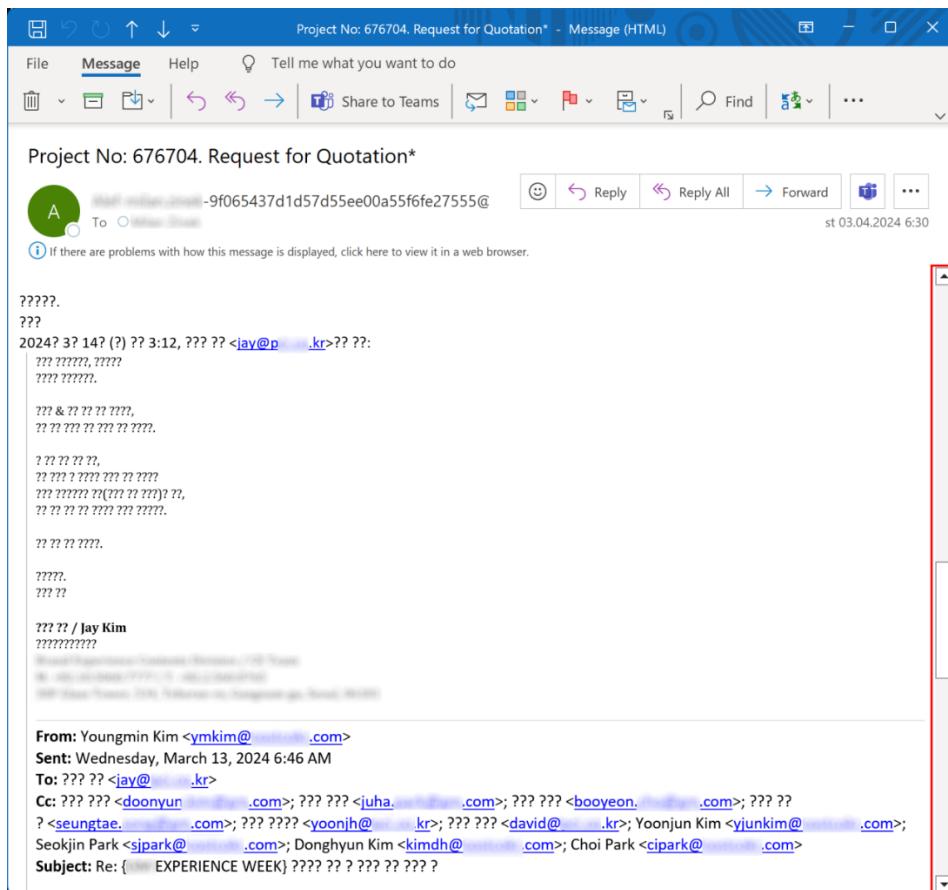
Here are a collection of recent attacks (generated by AI for training purposes).
If you look carefully then

1 Phishing via Email Chains & Hijacked Conversations (VERY common right now)

What Is Email Spoofing?



What does it look like?



The screenshot shows an email message in a Microsoft Outlook-style interface. The subject line is "Project No: 676704. Request for Quotation*". The message body is filled with numerous question marks, indicating a severely corrupted or garbled email. The recipient's name is partially visible as "jay@p... .kr". The message was sent on March 13, 2024, at 6:46 AM. The email header shows the following details:

From: Youngmin Kim <ymkim@... .com>
Sent: Wednesday, March 13, 2024 6:46 AM
To: ??? ??? <jay@... .kr>
Cc: ??? ??? <doonyun@... .com>; ??? ??? <juha@... .com>; ??? ??? <booveon@... .com>; ??? ??? <seungtae@... .com>; ??? ??? <yoonjh@... .kr>; ??? ??? <david@... .kr>; Yoonjun Kim <yjunkim@... .com>; Seokjin Park <sjpark@... .com>; Donghyun Kim <kimdh@... .com>; Choi Park <cipark@... .com>
Subject: Re: {... EXPERIENCE WEEK} ??? ??? ??? ??? ??? ???

From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2018 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com>
Subject: Please handle ASAP

– External email. Forward any suspicious emails to bad@yourcompany.com –

Hi James,

I'm currently tied up in a meeting for the next six hours, but we have a vendor saying we're late on paying an invoice. Can you handle the attached ASAP? I can't take calls, so just email me if you have questions.

Susan Fry
Chief Operating Officer
sfry@yourcompany.com

Sent from my iPhone, please excuse typos

🔴 Real-life example

An attacker compromises **one real mailbox** (often via password reuse).

They **reply inside an existing email thread** so it looks genuine.

Example:

“Hi, can you quickly check the attached updated drawing before today’s deadline?”

Halfway through the email chain:

- First emails: john.smith@company.co.uk
- Later reply: john.smith@company.co.uk
(The “a” is a different Unicode character — visually identical)

Or:

- @company.co.uk becomes @company-uk.co

👀 What users must watch for

Email thread suddenly:

- Asks for **urgent action**
- Includes a **new attachment or link**
- Mentions **payment, drawings, credentials, or access**

🚩 Red flags:

- Sender address **changes slightly mid-thread**
- Attachment type changes (PDF → ZIP → HTML)
- “Sent from iPhone” on messages that normally aren’t

⌚ What to do

Hover over sender email every time

If urgent or unusual → **verify via Teams / phone**

❌ Never open attachments just because it’s “part of a thread”

2 Fake Password Reset / MFA Prompts Outside Normal Cycles

How to mitigate MFA fatigue attacks



Create a strong password

Encourage reporting of suspicious activity

Monitor activity

Regular audits and improvements

Implement number matching in MFA applications

Contextual authentication

Use trustable MFA apps or devices

Regularly update devices and systems

User education and training

Limit authentication requests

Adaptive authentication

Use biometric authentication

What does this look like?

Microsoft account password reset  Inbox x

Microsoft account team <account-security-noreply@accountprotection.microsoft.com>
to me ▾

5:17 AM (

Microsoft account

Password reset code

Please use this code to reset the password for the Microsoft account Em*****@hotmail.com.

Here is your code: 

If you don't recognize the Microsoft account Em*****@hotmail.com, you can [click here](#) to remove your email address from that account.

Thanks,
The Microsoft account team



🔴 Real-life example

User gets:

- “Your password expires today”
- “Unusual sign-in detected”
- “MFA reset required”

But:

- It's **not** password-change week
- They weren't trying to log in
- The link goes to a **perfect Microsoft look-alike**

Attackers then:

- Capture the password
- Prompt for MFA
- Log in immediately

👀 What users must watch for

🚩 Password or MFA prompts when:

- You didn't request it
- It's **outside the normal monthly cycle**
- The link asks you to log in **again**

🚩 URLs like:

- microsoft-secure-login[.]com
- office365-verify[.]net

⌚ What to do

✓ **Never** click login links in emails

✓ Go directly to:

- portal.office.com
- your normal company login bookmark

✓ Report MFA prompts you didn't initiate **immediately**

3 Supplier / Finance Impersonation (Engineering firms are targets)

What does this look like?



From: Accounts <accounts@knownsupplier.com>
To: Accounts Payable <ap@recipientorg.com>
Subject: Change of bank details financial content
Attachments: invoice.16.21.pdf

Hi Devon,

Due to a change in our accounts system, we have changed our bank details as follows:

Account number: 1241249123 financial content

Please direct payment financial request for the invoice attached and all future invoices to the new account.

Regards,

Sam
Accounts Receivable



The screenshot shows an email message in Mozilla Thunderbird. The message is from 'Chee Sian <abby@lovong.com>' to 'To' (redacted). The subject is 'Bank Details'. The body of the email reads:

Good-Day,

We have tried to call your office today but no response,
we noticed your Invoice details do not bear your company's bank details,
as we intend to bank-in the payment for progress payment certificate for claim no. 5.

CLICK HERE TO FILL THE BANK DETAILS FORM

Please check above to reconfirm your company bank details ASAP and fill the bank details form above.
Waiting for Your Quick Response.

Regards,

Che Sian

CSCON SDN BHD (1214937-X)

CSTAN ENGINEERING (SA0169040-T)

33,JLN PEKAN BARU, TMN ENG ANN,
41150 KLANG,SELANGOR.

At the bottom, there is a note about attachments: '1 attachment: Bank Detail Form.pdf 153 KB' and a save button.

● **Real-life example**

Email claims to be from:

- A materials supplier
- CAD / software vendor
- Sub-contractor

“We’ve changed our bank details — please use the new account from today.”

The invoice looks real.

Logo, formatting, even previous invoice numbers copied.

● **What users must watch for**

▶ Any email asking to:

- Change bank details
- Re-pay an invoice
- Use “new” payment info urgently

▶ “This must be processed today”

○ **What to do**

✓ **Bank changes ALWAYS verified by phone**

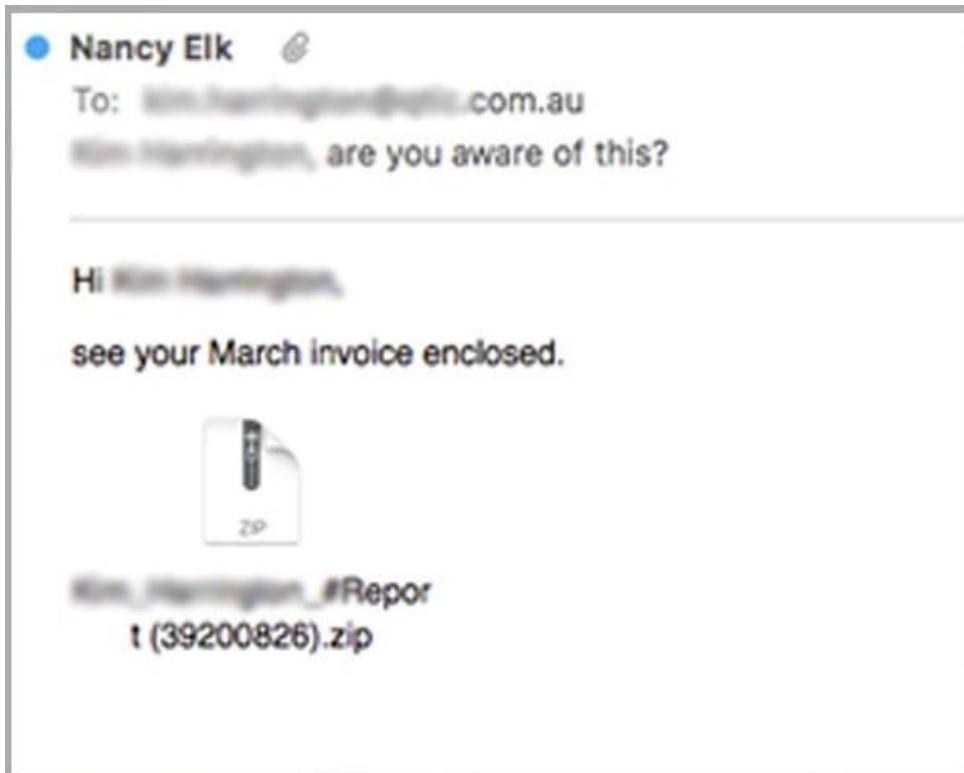
✓ Never trust bank changes by email alone

✓ Finance should already have a call-back rule

✓ Always check with a colleague for a second set of eyes

4 Malicious Attachments Disguised as “Drawings” or “Specs”

What does this look like?



PRICE UPDATE - Temporary Items

Message

PRICE UPDATE

SALES [REDACTED]

Tuesday, June 20, 2017 at 3:42 PM

To:

1 Attachment  Download All  Preview All

 PRICES UPDATE.html 9.1 KB

DEAR CUSTOMER,

PLEASE FIND THE ATTACHED UPDATE ON OUR PRICES.

THANKS.

● **Nancy Elk**

To: ...@...com.au

Hi ...@..., are you aware of this?

Hi ...@...,

see your March invoice enclosed.



[...@...#Report \(39200826\).zip](#)

● Real-life example

Attachment named:

- Drawing_Revision_7.zip
- Specs_Updated.html
- Quote_Confirmed.iso

User opens it → sees a fake login page or malware runs silently.

HTML files are especially dangerous — they open **locally** and steal credentials.

● What users must watch for

▶ Attachments ending in:

- .zip
- .html
- .iso
- .img

▶ Attachments requiring you to:

- “Enable content”
- “Sign in to view”

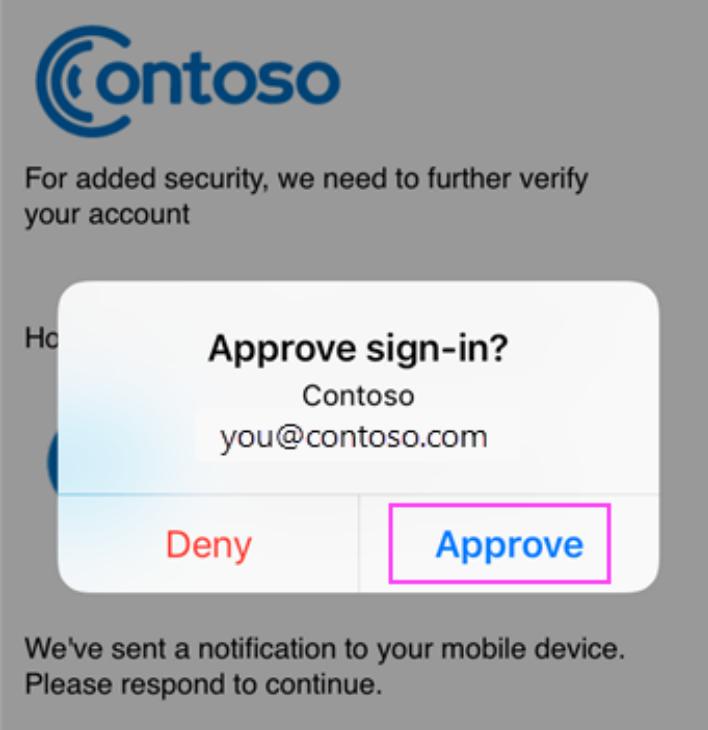
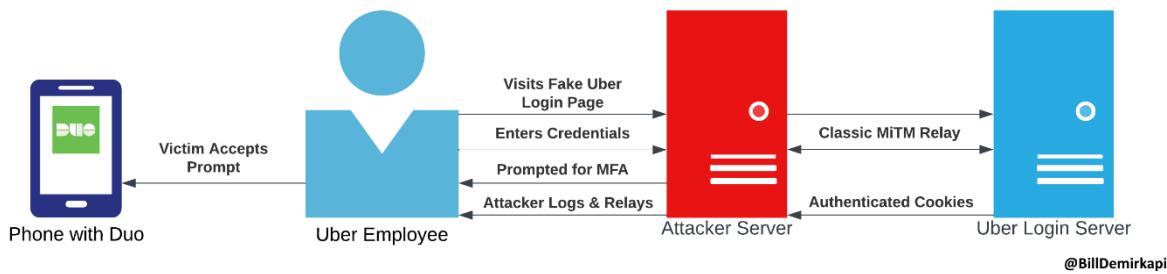
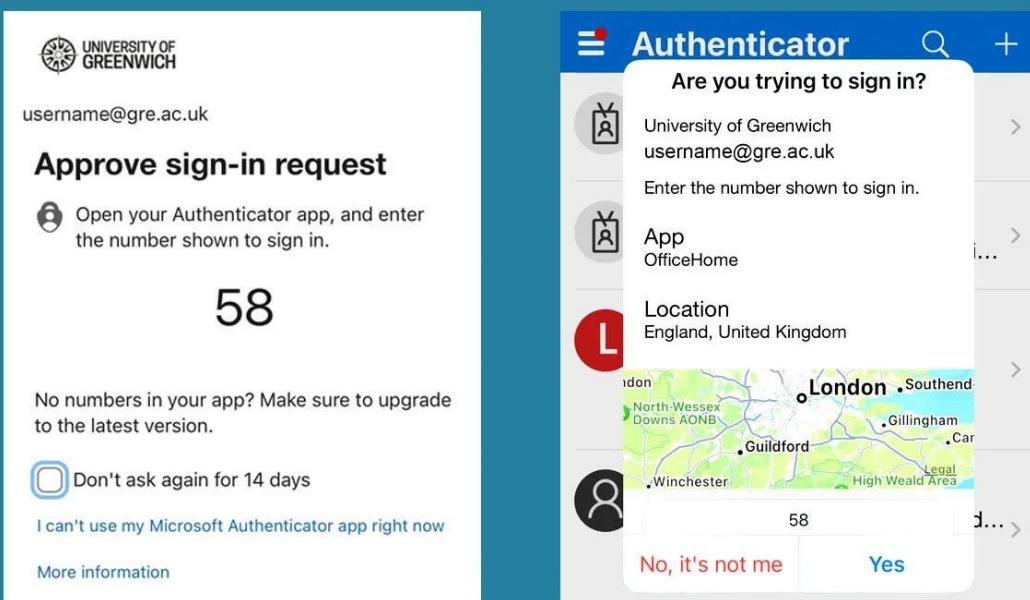
○ What to do

✓ Treat unexpected attachments as suspicious

✓ If in doubt → ask IT before opening

✗ Never enter passwords into files

5 MFA Fatigue & Push Bombing Attacks



supportdesk@andisa.net | 01423 290029 | www.andisa.net

🔴 Real-life example

Attacker already has your password.

They spam MFA requests until the user presses **Approve** just to stop the notifications.

👀 What users must watch for

🚩 Repeated MFA prompts when:

- You are NOT logging in
- They arrive late at night or early morning

⌚ What to do

✓ **Never approve unexpected MFA**

✓ Report immediately — this means your password is already compromised

✓ IT can block and reset before damage occurs

🧠 One-Minute Rule to Teach Users

If it's urgent, unexpected, or asks for credentials — stop and verify.

Always pause if:

- Someone pressures urgency
- Login is requested unexpectedly
- Payment details change
- Attachments aren't expected
