# Assignment Questions-14

*1. Choose a fake profile on any social media platform of your preference and identify the red flags signaling its fraudulent nature.*

ANS:

Knowing how to spot a fake profile can go far in protecting you and your loved ones against online exploitation. Online predators commonly hide behind fake social media profiles, creating accounts by using fake names and bios designed to appeal to their preferred victims. Creating these accounts simply requires an email address, a phone or computer, and takes less than 2 minutes. With the click of an "Accept Request" button, they gain access to their target's profile. Here, the grooming process begins, and underage victims may be vulnerable to the manipulation and control of experienced predators.

1. **Friends Check:** Social media was designed for social interaction. Make sure the profile has a normal number of friends or followers. Profiles with under 100 friends are highly suspicious, especially if the account allegedly belongs to a teen.
2. **Photo Check:** Profiles without a profile photo are almost always spam or fake accounts. Profiles with none or only a few posted photos of themselves in social situations should raise your alarm.
3. **Status Check:** Profiles with minimal status updates or comments should be looked at as suspicious accounts. Again, the purpose of social media is to be social. Having a private account is common. But accounts with whom you are "friends" with should show social interaction beyond just that profile and your profile, or your child's profile. If there is only isolated interaction, then it is likely that account was created solely for interaction with you or your child.

4. **Surname Check:** If an account's "friends" list is visible, check for other "friends" with the same last name of the account holder (if known). If the account holder does not have connections with other people using the same last name, it may be a fake account.

5. **Birthday Check:** Many social media networks allow you to search posts for a specific profile. For instance, Facebook has a "search" function which is visible from most profiles once you navigate to their main page and click on "search profile". One of the most common social interactions is birthdays. Simply typing in "Happy Birthday" or "HBD" should bring up all posts and/or comments related to birthdays. (This search capability can be disabled by users).

6. **Reverse Image Check:** If a profile has only a few photos or you feel as though the account may be suspicious or fake, a quick reverse image search of some of the photos may be useful. This can be done by downloading or saving the published photos. Once saved, navigate to www.google.com/imghp. This is the Google photos page. Drag the photo into the google search bar or click the "browse" button and navigate to the saved photo. Within seconds, google will return results if that photo is found elsewhere on the internet. If the photo is visible on other accounts using a different name or appears to be from a commercial website, the profile is most likely a fake account.

7. **Username Check:** Profile names and account usernames can be different. For instance, Facebook allows users to create a "vanity URL" for their page if they desire. If a vanity URL is created the profile page might display the name "John Smith" but the account's official username may be "johnny.davis.0001". This can easily be identified by checking the URL or web address of the profile page visible in your internet browser (www.Facebook.com/johnny.davis.0001). This is similar for other social media networks. Users can display a name on their profile, but their actual account username may differ. Once an accounts unique username is identified, a quick Google search of that username may lead you to other social media accounts or to comments/complaints

related to suspicious activity. When searching usernames on Google be sure to place the username within quotes (“username.123” or “@username.123”) depending on the social media network. Discrepancies with usernames often indicate a fake account.

*2. Outline the objectives and demographics of Interpol's International Child Sexual Exploitation Database.*

ANS:

**The study identified a number of alarming trends:**

- The younger the victim, the more severe the abuse.
- 84% of images contained explicit sexual activity.
- More than 60% of unidentified victims were prepubescent, including infants and toddlers.
- 65% of unidentified victims were girls.
- Severe abuse images were likely to feature boys.
- 92% of visible offenders were male.

*3. Identify five suspicious SMS/emails you've received, cross-reference the sender phone no. or email against the NCRP Suspect database, and present the findings.*

ANS:

**1. The message is sent from a public email domain**

No legitimate organisation will send emails from an address that ends ‘@gmail.com’.

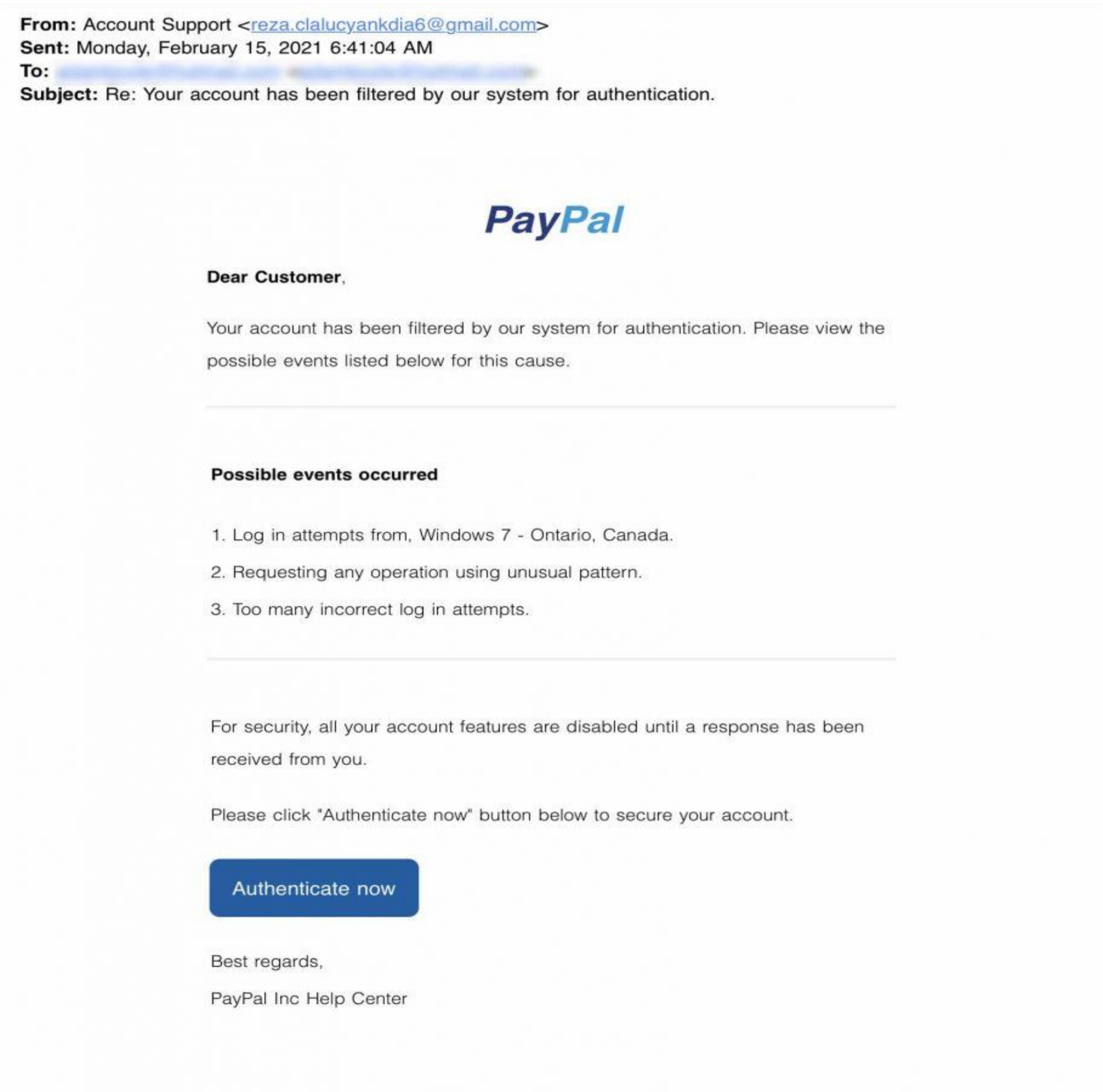
Not even Google.

Except for some small operations, most companies will have their own email domain and email accounts. For example, genuine emails from Google will read ‘@google.com’.

If the domain name (the bit after the  @ symbol) matches the apparent sender of the email, the message is probably legitimate.

By contrast, if the email comes from an address that isn’t affiliated with the apparent sender, it’s almost certainly a scam.

The most obvious way to spot a bogus email is if the sender uses a public email domain, such as ‘@gmail.com’.



**From:** Account Support <reza.clalucyankdia6@gmail.com>
**Sent:** Monday, February 15, 2021 6:41:04 AM
**To:** [redacted]
**Subject:** Re: Your account has been filtered by our system for authentication.

PayPal

**Dear Customer**,

Your account has been filtered by our system for authentication. Please view the possible events listed below for this cause.

**Possible events occurred**

1. Log in attempts from, Windows 7 - Ontario, Canada.
2. Requesting any operation using unusual pattern.
3. Too many incorrect log in attempts.

For security, all your account features are disabled until a response has been received from you.

Please click "Authenticate now" button below to secure your account.

Best regards,
PayPal Inc Help Center

In this example, you can see that the sender’s email address doesn’t align with the message’s content, which appears to be from PayPal.

However, the message itself looks realistic, and the attacker has customised the sender’s name field so that it will appear in recipients’ inboxes as ‘Account Support’.

Other phishing emails will take a more sophisticated approach by including the organisation's name in the local part of the domain. In this instance, the address might read 'paypalsupport@gmail.com'.

At first glance, you might see the word 'PayPal' in the email address and assume it is legitimate. However, you should remember that the important part of the address is what comes after the @ symbol. This dictates the organisation from which the email has been sent.

If the email is from '@gmail.com' or another public domain, you can be sure it has come from a personal account.

### 2. The domain name is misspelt

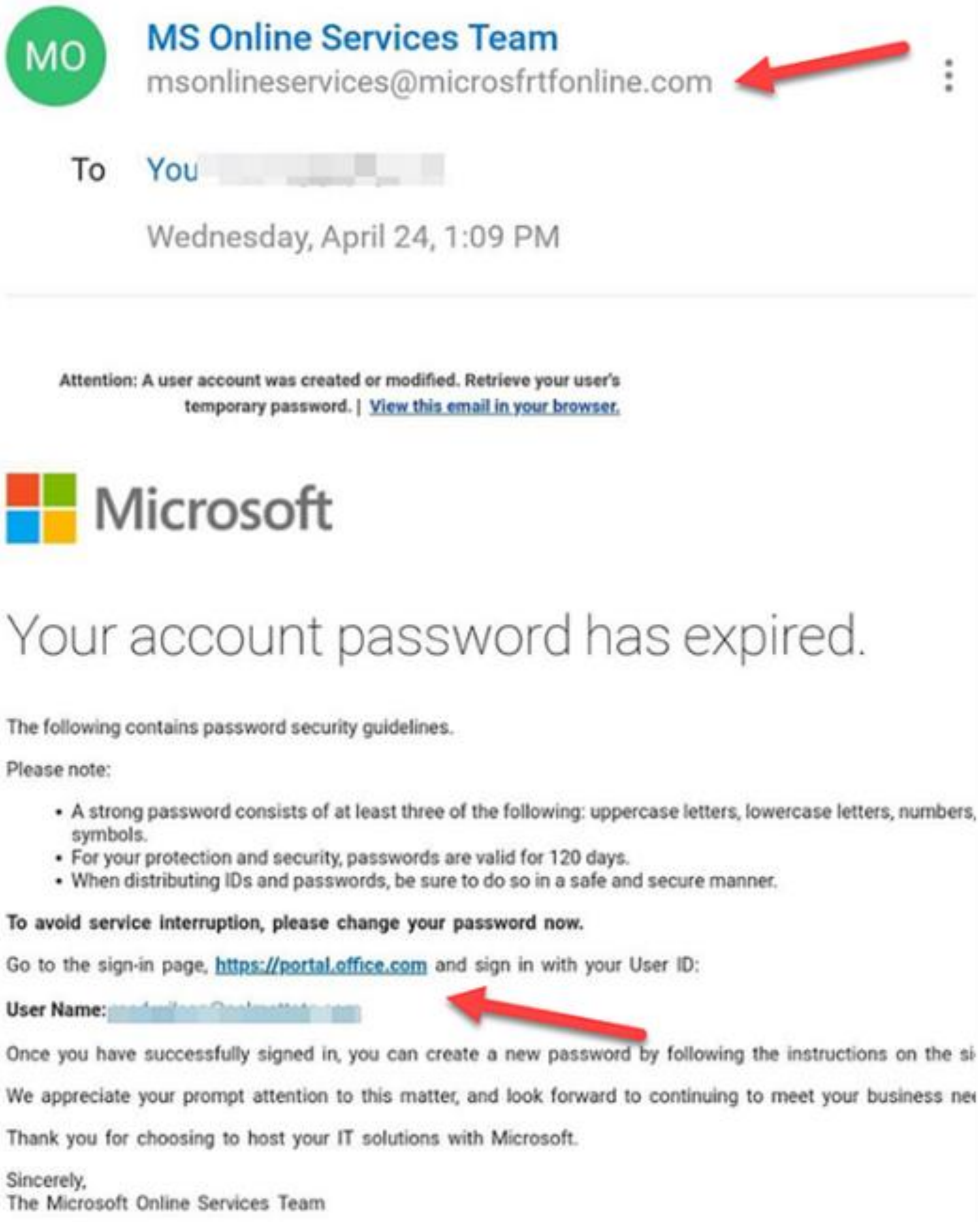
There's another clue hidden in domain names that provides a strong indication of phishing scams – unfortunately, it complicates our previous clue.

The problem is that anyone can buy a domain name from a registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed.

Here, scammers have registered the domain 'microsfrtfonline.com', which to a casual reader mimics the words 'Microsoft Online', which could reasonably be considered a legitimate address.

Meanwhile, some fraudsters get even more creative. The Gimlet Media podcast 'Reply All' demonstrated that in the episode What Kind Of Idiot Gets Phished?.
Phia Bennin, the show's producer, hired an ethical hacker to phish various employees. He bought the domain 'gimletrnedia.com' (that's r-n-e-d-i-a, rather than m-e-d-i-a) and impersonated Bennin.

Take a look at this example:



MS Online Services Team
msonlineservices@microsfrtfonline.com

To You [redacted]

Wednesday, April 24, 1:09 PM

Attention: A user account was created or modified. Retrieve your user's temporary password. | View this email in your browser.

Microsoft

Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, symbols.
- For your protection and security, passwords are valid for 120 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

**To avoid service interruption, please change your password now.**

Go to the sign-in page, https://portal.office.com and sign in with your User ID:

**User Name:** [redacted]

Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business ne

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team

His scam was so successful that he tricked the show's hosts, Gimlet Media's CEO and its president.

As Bennin went on to explain, you don’t even need to fall victim for a criminal hacker to gain vital information.

In this scam, the ethical hacker, Daniel Boteanu, could see when the link was clicked, and in one example, that it had been opened multiple times on different devices.

He reasoned that the target’s curiosity kept bringing him back to the link but that he was suspicious enough not to follow its instructions.

### 3. The email is poorly written

You can often tell if an email is a scam if it contains poor spelling and grammar.

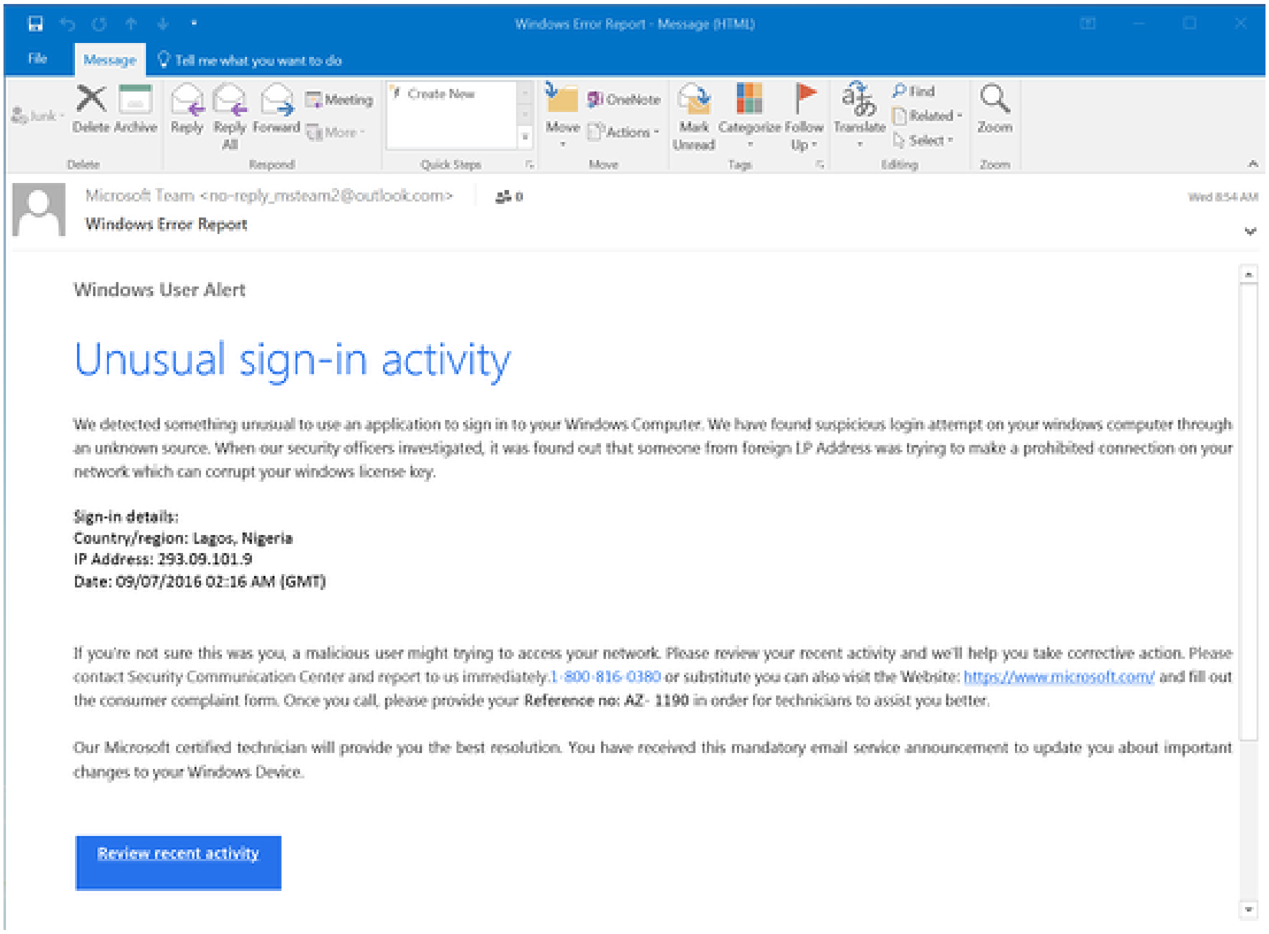
Many people will tell you that such errors are part of a ‘filtering system’ in which cyber criminals target only the most gullible people.

The theory is that if someone ignores clues about how the message is written, they’re less likely to pick up clues during the scammer’s endgame.

However, this only applies to outlandish schemes like the oft-mocked Nigerian prince scam, to which you must be incredibly naive to fall victim.

That, and scams like it, are manually operated: once someone takes to the bait, the scammer has to reply. As such, it benefits the crooks to ensure the pool of respondents contains only those who might believe the rest of the con.

take this example of a scam imitating Windows:



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

**Sign-in details:**
**Country/region: Lagos, Nigeria**
**IP Address: 293.09.101.9**
**Date: 09/07/2016 02:16 AM (GMT)**

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

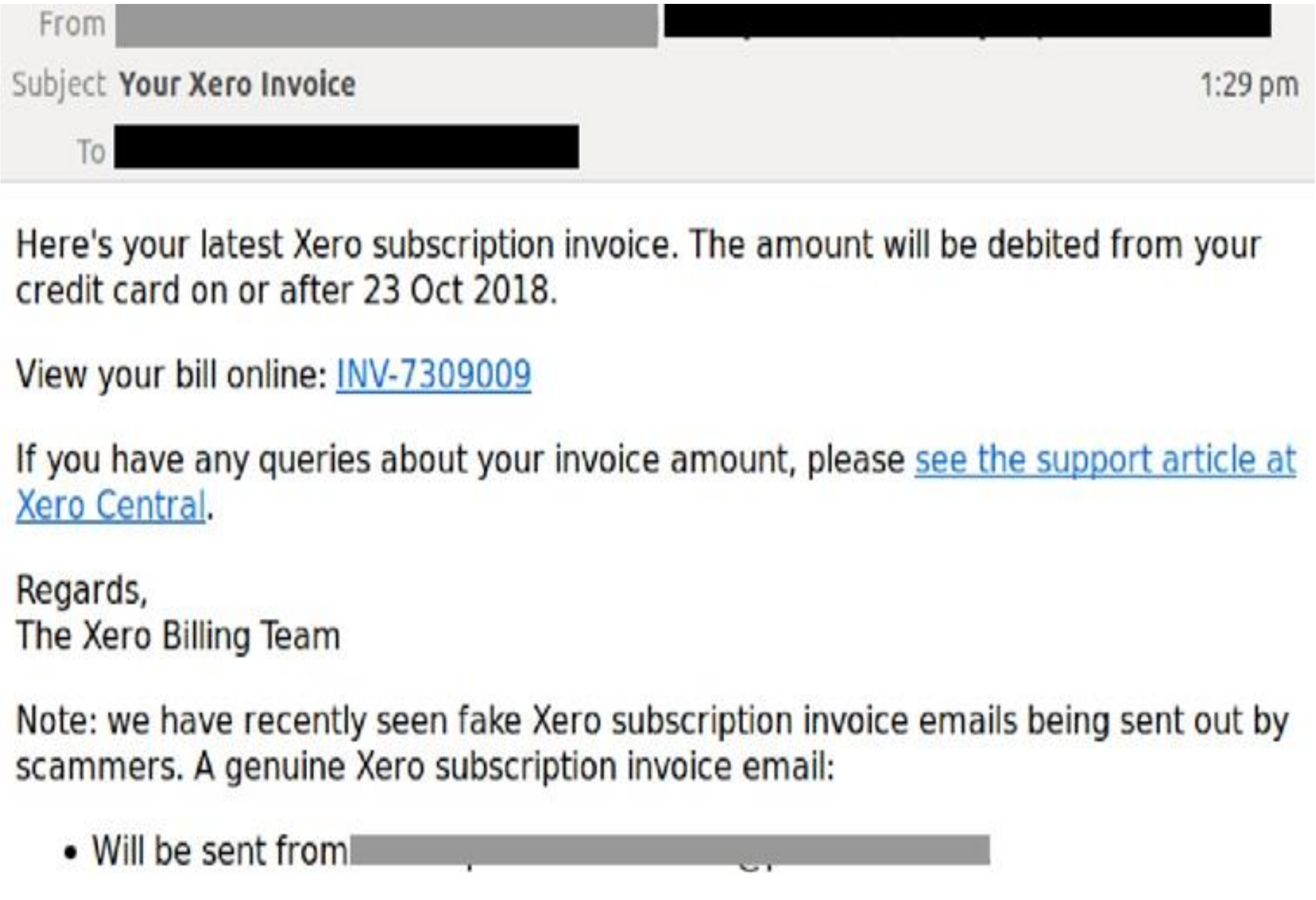
## 4. It includes suspicious attachments or links

Phishing emails come in many forms. We've focused on emails in this article, but you might also get scam text messages, phone calls or social media posts.

But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment you're asked to download or a link to a bogus website.

The purpose of these payloads is to capture sensitive information, such as login credentials, credit card details, phone numbers and account numbers.

In a typical example, like the one below, the phisher claims to be sending an invoice:



From [redacted]
Subject **Your Xero Invoice** 1:29 pm
To [redacted]

Here's your latest Xero subscription invoice. The amount will be debited from your credit card on or after 23 Oct 2018.

View your bill online: INV-7309009

If you have any queries about your invoice amount, please see the support article at Xero Central.

Regards,
The Xero Billing Team

Note: we have recently seen fake Xero subscription invoice emails being sent out by scammers. A genuine Xero subscription invoice email:

- Will be sent from [redacted]

**5. The message creates a sense of urgency**

Scammers know that most of us procrastinate. We receive an email giving us important news, and we decide we'll deal with it later.

But the longer you think about something, the more likely you will notice things that don't seem right.

Maybe you realise that the organisation doesn't contact you by that email address, or you speak to a colleague and learn that they didn't send you a document.

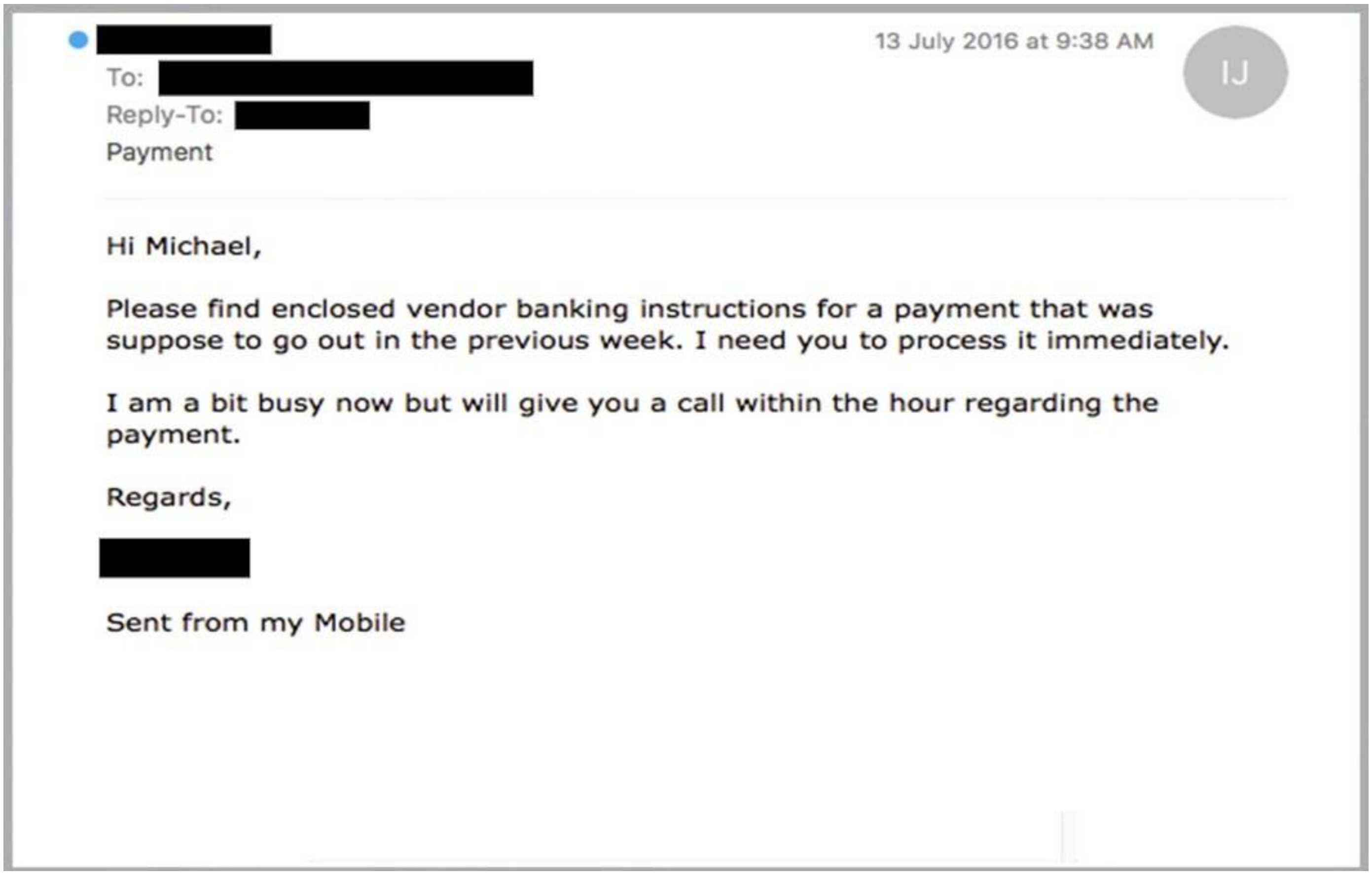
Even if you don't get that 'a-ha' moment, returning to the message with a fresh set of eyes might help reveal its true nature.

That's why so many scams request that you act now, or else it will be too late. This has been evident in every example we've used so far.

PayPal, Windows and Netflix provide regularly used services, and any problems with those statements could cause immediate inconveniences.

The manufactured sense of urgency is equally effective in workplace scams.

A typical example looks like this:



[redacted]

13 July 2016 at 9:38 AM

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

**Prevent phishing by educating your employees**

The best way to protect your business from phishing scams is to educate employees about how they work and what to look out for.

Regular staff awareness training will ensure that employees know how to spot a phishing email, even as fraudsters' techniques become increasingly more advanced.

It's only by reinforcing advice on avoiding scams that your team can develop good habits and detect detect signs of a phishing email as second nature.

## *4. What are the guidelines to be followed by children while accessing public systems, as per ISEA portal ([www.infosecawareness.in](www.infosecawareness.in))?*

*ANS:*

Few tips to enable privacy and security features on digital devices for safety and protection:

- **Authentication for accessing mobile** with finger print or Face recognition and a lock screen with a pattern pass code or a password is necessary to avoid misuse of the mobile.

  Steps to enable biometric authentication and passwords: Authentication - 1- settings; 2 - lockscreen and password
- **Enable google play protect** on your mobile. It scans your mobile and alerts you on signs of misbehaving apps or anything suspicious. Confirm and make sure it is working by checking if it is active.

  Steps to enable google play protect :

  1- googleplay store ; 2- at the top right tap the profile icon; 3- click on play protect ;3 - check wether option is enabled n active
- **Enable find my device option** to trace your mobile device by finding its exact location of the on an interactive map.

Steps to enable find my device option:

1 - settings ; 2 - google ; 3 - security ; 4- enable find my device

- **Update emergency contact information** on your mobile to display the contact number on lock screen in case of emergency.

  How to set up an Android emergency contact

  There are a couple of ways to set up ICE contact information on an Android phone. First, you can add your info to the emergency information feature:

1. Open the “Settings” app.Tap “User & accounts,” then “Emergency information.”
2. To enter medical information, tap “Edit information” (you might have to tap “Info” first, depending on the version).
3. There’s a separate section where you can enter emergency contacts; tap “Add contact” to add a person from your contacts list (you might have to tap “Contacts” first)

- **Enable 2 factor authentication** to rule out the possibility of misuse or theft of passwords. This feature ensures another layer of security.

  Steps to enable 2factor authentication option: (On your Android phone or tablet)

  1- Settings app; 2 - Google; 3 - Manage your Google Account; 4- click security; 5- enable 2 step verification and enable options

- **Enable safe browsing options on your mobile** to get a warning on trying to access or open a malicious site or download dangerous content. Chrome is a default android browser that is enabled with safe browsing feature.

  Steps to enable safe bowsing option on your mobile

  1- click on chrome; 2-go to settings/ tap the profile icon on top right ; 3 - privacy ; 4 - enable safe browsing

- **Use Youtube kids app for safely viewing youtube videos**

  This is a free downloadable app that is created by YouTube for kids. It allows parents the option to set an age level of their child to view only specific related content that has been reviewed by Google and marked as appropriate for that age group.

  For using it-

- download the app from playstore into your device
- set it up for your child by entering the year of birth, choosing appropriate age group and other options,
- after you enter your email and send parental consent,
- you receive 4 digit verification code
- using the code you can start using this app for your child on the device. (this is available on ios and android devices)

Other options to view youtube safely especially for children–

**-Watch and share videos on safeyoutube.net**

This is another solution to watch and share youtube videos without any other distracting content in view.

https:/ /safeyoutube.net/w/xOxE

To use the safeyoutube.net –

- copy the url of the youtube video that you want to share or watch,
- later paste it on the on the website safeyoutube.net in the option given for 'Generate your safe YouTube link'
- once you generate the link you can use or share this safe link for viewing the youtube videos without any other content or advtertisements appearing on the screen.

***5. Go through CIS Google Android Benchmark document and provide a brief overview on the privacy and browser configuration settings suggested.***

***Ans:***

## ***Privacy settings***

**(L1)  Ensure 'Lock screen' is set to 'Don't show notifications at all' (Manual)**

Profile Applicability:

- Level 1

Description: Disable notifications on the lock screen. The recommended state for this setting is: Don't show notifications at all.

Rationale:

If the device is lost or unattended, disabling notifications prevents the information from appearing on the lock screen. This information might be confidential, and thus unwarranted disclosures could be avoided.

Impact:

The user will not see the contents of notifications on the lock screen, requiring the user to unlock the device each time.

Audit:

To verify notifications on the lock screen are not shown:

1. Tap Settings Gear Icon.

2. Tap Apps & notifications.

3. Tap Notifications.

4. Tap Advanced.

5. Tap Lock Screen.

6. Verify that Lock Screen is set to Don't show notifications at all.

Remediation:

Follow these steps to set the lock screen to show no notifications:

1. Tap Settings Gear Icon.

2. Tap Apps & notifications.

3. Tap Notifications.

4. Tap Advanced.

5. Tap Lock Screen.

6. Tap Lock Screen and set it to Don't show notifications at all.

**(L2) Ensure 'Use location' is set to 'Disabled' (Manual)**

Profile Applicability:

• Level 2 Description:

Disable Location when not in use.

The recommended state for this setting is: Disabled.

Rationale:

Enabling a device's location allows applications to gather and use data showing the user’s location. The user’s location is determined by using available information from cellular network data, local Wi-Fi networks, Bluetooth, and GPS. If the user turns off Location Services, the user will be prompted to re-enable location the next time an application tries to use this feature.

Disabling location reduces the capability of an attacker to determine or track the user’s location via websites, locally installed applications, or other means without the user’s consent. Thus, it should be disabled when not in use.

Note: Location is significant for tracking the lost device if the device data is not disabled. Make an informed decision to determine what is best for the organization.

Impact:

Each time an application needs location data, the user activity would be interrupted to enable the location manually. Additionally, if the device is lost and the location is disabled, A user cannot use remote locate services such as Android Device Manager.

Audit:

Follow the below steps to verify that Use location is Disabled:

1. Tap Settings Gear Icon.

2. Tap Location.

3. Verify that Use location is OFF.

Remediation:

Follow the below steps to disable Use location:

1. Tap Settings Gear Icon.

2. Tap Location.

3. Toggle Use Location switch to the OFF position.

## ***Browser configuration settings***

**(L1) Ensure 'Microphone' is set to 'Enabled' (Manual) Profile Applicability:**

- Level 1

Description:

This setting controls if a site asks before accessing the microphone. The recommended state for this setting is: Enabled. Rationale: Websites will have to ask permission before being allowed to access the microphone, which will help prevent unwanted access to the microphone and help protect against potential privacy concerns. Impact: Users will be prompted each time a website requests access to the microphone.

Audit: Follow the below steps to verify that Microphone is Enabled:

1. Tap Chrome Icon.

2. Tap Menu Icon.

3. Tap Settings.

4. Tap Site settings.

5. Verify that Microphone displays Ask first.

Remediation:

Follow the below steps to Enable the Microphone permission request:

1. Tap Chrome Icon.

2. Tap Menu Icon.

3. Tap Settings.

4. Tap Site settings.

5. Tap Microphone.

6. Toggle to the ON position. Default Value: Enabled.

**(L1) Ensure 'Location' is set to 'Enabled' (Manual) Profile Applicability:**

- Level 1

Description:

This setting controls if a site asks before accessing the location. The recommended state for this setting is: Enabled.

Rationale: Websites will have to ask permission before being allowed to access the location, which will help prevent unwanted access to the user's location and help protect against potential privacy concerns.

Impact:

Users will be prompted each time a website requests access to the location. Audit: Follow the below steps to verify that Location is Enabled:

1. Tap Chrome Icon.

2. Tap Menu Icon.

3. Tap Settings.

4. Tap Site settings.

5. Verify that Location displays Ask first.

Remediation:

Follow the below steps to Enable the Location permission request:

1. Tap Chrome Icon.

2. Tap Menu Icon.

3. Tap Settings.

4. Tap Site settings.

5. Tap Location.

6. Toggle to the ON position. Default Value: Enabled.