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

ANSWER:

Understanding Fake Profiles

Understanding fake profiles involves recognising that they are deceptive online personas created by individuals hiding their true identity.

These profiles can range from harmless pseudonyms to malicious impersonations used for fraud, bullying, or identity theft.

They often feature fabricated details, such as unrealistic photos or inconsistent backstories.

The motives behind creating false accounts vary, including personal amusement, the desire to spy on others, or more sinister intentions like scamming unsuspecting victims.

Identifying these profiles requires vigilance and a keen eye for details that don't add up, as they can have significant real-world consequences despite their virtual nature.

Signs of a Fake Profile

Signs of a fake acounts often include a combination of unusual patterns and inconsistencies that stand out upon closer inspection. Here are some key indicators:

1. ***Limited Profile Information***: Fake profiles typically have minimal personal information, vague biographies, or incomplete details.
2. ***Unrealistic Photos***: They often use stock images or photos of celebrities as profile pictures. Sometimes, the images look overly edited or too professional for a regular social media account.
3. ***Inconsistent Posting***: The posting history might be erratic or non-existent. Posts may lack personal touches or have a generic feel.
4. ***Few Friends or Followers***: These profiles usually have a very low number of friends or followers, or conversely, an unusually high number with little interaction.
5. ***Rapid Friend Requests***: Sending friend requests en masse in a short period is a common trait of fake profiles.
6. ***Lack of Personal Interaction***: There's often little to no engagement with others in comments or posts.
7. ***Requesting Personal Information***: They may quickly move to ask for personal or sensitive information.
8. ***Spammy Links or Messages***: Sharing unsolicited links or sending spam messages is a red flag.

9. ***Inconsistencies in Stories***: *The details shared by the user might contradict over time.*
10. ***New Account***: *Many fake profiles are relatively new with a recent creation date.*

Being aware of these signs can help in identifying and avoiding potential scams or deceptive interactions online.

Impact of Fake Accounts on Brands

The impact of counterfeit profiles, often referred to as bogus or sham accounts, on brands can be significant and multifaceted.

These deceptive online personas can harm a brand's reputation, customer trust, and even financial health. Here are some ways they affect brands:

1. ***Brand Reputation Damage***: *Imposter accounts can spread misinformation or negative comments about a brand, tarnishing its public image and reputation.*
2. ***Misleading Metrics***: *Brands often rely on social platforms metrics for marketing strategies. Fake accounts skew these metrics, leading to inaccurate data analysis and marketing decisions.*
3. ***Customer Trust Erosion***: *When customers encounter fraudulent profiles pretending to be a brand, their trust in the brand can be severely damaged, especially if they fall victim to scams under the brand's guise.*
4. ***Increased Marketing Costs***: *Dealing with the fallout of sham profiles often requires additional resources, increasing marketing and public relations costs.*
5. ***Competitive Disadvantage***: *Competitors might use dummy profiles to engage in unfair practices like posting negative reviews or spreading false information about a brand.*
6. ***Legal and Compliance Issues***: *Brands may face legal challenges if counterfeit profiles engage in illegal activities, like selling counterfeit products, under their name.*
7. ***Customer Service Challenges***: *Responding to queries or complaints originating from phony accounts can drain customer service resources.*
8. ***Infiltration of Customer Communities***: *Fake profiles can infiltrate brand communities, spreading discord or false information among genuine customers.*
9. ***Ad Fraud***: *Brands may waste advertising budgets targeting these non-existent users, leading to poor return on investment.*
10. ***Intellectual Property Theft***: *Some fake profiles might illegally use a brand's intellectual property, misleading consumers and diluting the brand's value.*

In summary, the presence of counterfeit profiles can have a profound and negative impact on a brand's integrity, customer relationships, and overall business performance.

It's crucial for brands to actively monitor and address these fraudulent activities to protect their reputation and maintain customer trust.

Strategies for Brands: How to Confront Someone with a Fake Profile Online

Confronting someone with a fake profile online, particularly when it's crucial for safeguarding your brand, demands a strategic and careful approach.

Here's a guide on how to navigate this complex situation:

1. ***Gather Evidence**: Collect all interactions and evidence indicating the profile is fake and harmful to your brand. This includes screenshots of the profile, messages, posts, and any other relevant information. Pay special attention to profile photos and the follower list, which might give away a fake identity.*
2. ***Verify the Profile's Authenticity**: Before taking action, confirm the profile's authenticity. A seemingly fake profile might be a real person with similar branding or a misunderstanding.*
3. ***Reach Out Privately**: Contact the individual behind the fake profile privately, if possible. Approach the conversation with professionalism, expressing your concerns about the potential impact on your brand.*
4. ***State Your Case Clearly**: Clearly articulate why you believe the profile is fake and its effect on your brand. Specify the harm, whether it's spreading misinformation, tarnishing your reputation, or misleading customers.*
5. ***Seek a Peaceful Resolution**: Urge the person to voluntarily remove the harmful content. Some individuals may not realise the damage they're causing and might be willing to resolve the situation amicably.*
6. ***Use Legal and Platform Channels**: If the individual is uncooperative, report the fake account through the social media network's reporting mechanisms. Consider legal action if there's significant brand damage or financial loss.*
7. ***Communicate with Your Audience**: Inform your audience about the fake social accounts to avoid confusion. Maintaining transparency can help protect your brand's reputation.*
8. ***Monitor Your Brand Regularly**: Continuously monitor your brand online using social media monitoring tools to detect other fake or copycat accounts.*
9. ***Educate Your Audience**: Share tips with your audience on identifying authentic communications from your brand, focusing on the authenticity of profiles and distinguishing between legitimate accounts and artificial accounts or anonymous accounts.*
10. ***Strengthen Your Online Presence**: Enhance your official profiles with authentic content to overshadow any false profiles or broader network of bots.*

Remember, while it's crucial to confront someone with a fake social media profile to protect your brand, it's equally important to handle the situation tactfully to prevent escalating the issue or further damaging your brand's reputation.

In the realm of social media platforms, particularly Facebook, distinguishing genuine engagement from interactions driven by fake profiles is crucial for understanding the true impact of your content.

Here's a guide to help you discern and mitigate the influence of these inauthentic profiles on your Facebook posts:

1. ***Analyse Engagement Metrics**: Scrutinise the engagement metrics of your posts. Disproportionately high engagement paired with low conversion rates or superficial interactions often signals interactions from harmful bot accounts or non-genuine profiles.*
2. ***Inspect Follower List**: Regularly examine your follower counts. Be wary of profiles that lack a profile photo, display minimal personal information, or were created very recently, as these could be indicators of fake accounts.*
3. ***Utilise Facebook Insights**: Leverage Facebook Insights for comprehensive analytics on your audience. Sudden spikes in follower counts from regions outside your target market may suggest the presence of fake profiles.*
4. ***Monitor Comments and Reactions**: Assess the authenticity of the online accounts engaging with your posts. Fake profiles typically leave kinds of comments that are generic and unrelated to the content on the profile.*
5. ***Employ Advanced Analytics Tools**: Incorporate third-party tools that specialise in detecting fake profiles and inauthentic activities. These tools often provide deeper insights than standard social network analytics.*
6. ***Report and Remove Suspicious Followers**: Proactively report and block suspicious profiles. This action helps in maintaining the authenticity of your audience and ensures engagement with real users.*
7. ***Refine Your Audience Targeting**: When creating ads or boosted posts, narrowly define your target audience. This precision minimises the chances of your content reaching fake profiles or bots.*
8. ***Educate Your Followers**: Inform your genuine followers about the prevalence of fake profiles. Encourage them to exercise caution when interacting with questionable accounts, addressing Internet Matters and cyber issues related to online safety.*
9. ***Conduct Regular Content Audits**: Periodically review your content to identify which types resonate with actual persons. Adjusting your content strategy based on these insights can organically diminish the influence of fake accounts.*
10. ***Stay Informed on Facebook's Policies**: Keep abreast of the latest policies and tools provided by Facebook to combat fake accounts and harmful activity. Utilising these resources can significantly bolster your defense against inauthentic engagements.*

By actively managing your presence on social media sites like Facebook, you can effectively reduce the reach and impact of fake accounts on your posts, ensuring more authentic and meaningful interactions with your audience.

Conclusion

Confronting someone with a fake profile online requires a nuanced approach, especially on social platforms where fake photos, identical images, and false messages are prevalent.

It's about distinguishing genuine people from fake followers and discerning human activity from automated responses.

Addressing this issue often involves tackling common questions about authenticity and being aware of tactics like the fishing technique used by imposters.

By staying vigilant and informed, we can better navigate these challenges and maintain the integrity of our online interactions, ensuring a safer and more trustworthy digital environment for all.

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

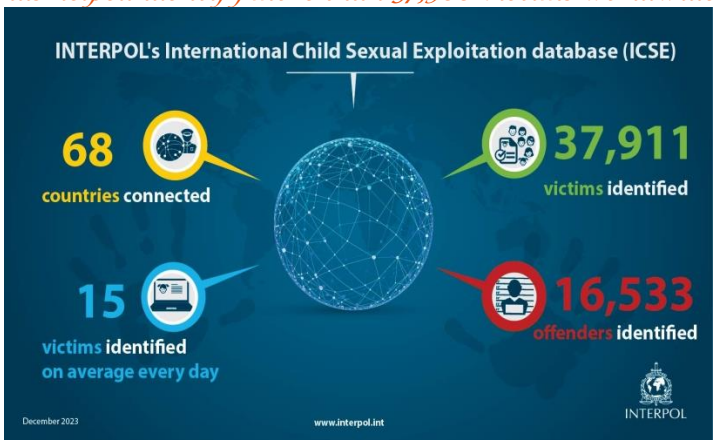
Our International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool, which allows specialized investigators to share data on cases of child sexual abuse.

Using image and video comparison software, investigators are instantly able to make connections between victims, abusers and places. The database avoids duplication of effort and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images.

It also allows specialized investigators from more than 68 countries to exchange information and share data with their colleagues across the world.

By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate victims of child sexual abuse.

INTERPOL's Child Sexual Exploitation database holds more than 4.9 million images and videos and has helped identify more than 37,900 victims worldwide.



Young victims, severe abuse

Most people don't realize that when we talk about child sexual abuse, this includes the abuse of very young children, and even babies.

Following the examination of random selection of videos and images in the ICSE database, INTERPOL and ECPAT International published a joint report in February 2018 entitled Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material.

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

.

Email phishing is one of the most frequent forms of cyber crime, but despite how much we think we know about these scams, they still catch us out all too often.
According to Proofpoint's 2022 State of the Phish Report, 83% of organisations fell victim to a phishing attack last year.
Meanwhile, Verizon's 2021 Data Breach Investigations Report found that 25% of all data breaches involve phishing.
These figures help explain why phishing is considered to be among the biggest cyber security risks that organisations face. With a single email, criminal hackers can steal our personal information or infect our devices with malware.

Fortunately, preventing these attacks can be as simple as knowing how to identify phishing emails.

But how do you spot a scam email? This blog uses five real-life examples to demonstrate the common signs that someone is trying to scam you.

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'.

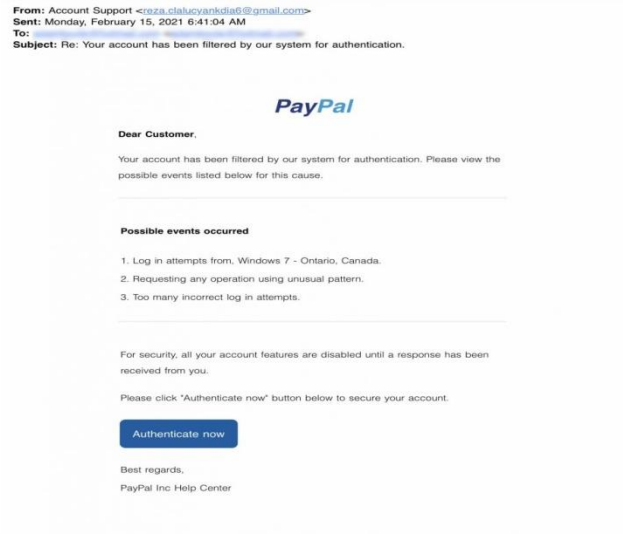


Image: Pickr

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.

Take a look at this example:

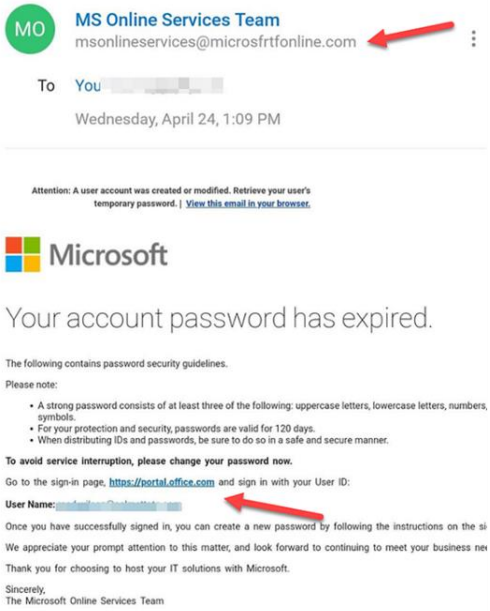


Image: PTG
Here, scammers have registered the domain 'microsfrtfonline.com', which to a casual reader mimics the words 'Microsoft Online', which could reasonably be considered a legitimate address.

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.

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.

Boteanu explains:

I'm guessing [the target] saw that something was going on, and he started digging a bit deeper and [...] trying to find out what happened [...]
And I'm suspecting that after, [the target] maybe sent an email internally saying, "Hey guys! This is what I got. Just be careful. Don't click on this [...] email.
Boteanu's theory is precisely what happened. But why does that help the hacker? Bennin elaborates:

The reason Daniel had thought [the target] had done that is because he had sent the same email to a bunch of members of the team, and after [the target] looked at it for the fourth time, nobody else clicked on it.
And that's okay for Daniel because he can try, like, all different methods of phishing the team, and he can try it a bunch of different times. [And] since [the target is] sounding alarm bells, he probably won't include [him] in the next phishing attempt.
Therefore, criminal hackers often still win even when you've thwarted their initial attempt.

That is to say, indecisiveness in spotting a phishing scam provides clues to the scammer about where the strengths and weaknesses in your organisation are.

Launching subsequent scams that use this information takes minimal effort, and they can keep doing this until they find someone who falls victim.

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.

But this doesn't apply to phishing.

See also:

- The effects of phishing awareness training wear off over time
- Phishing attacks: 6 reasons why we keep taking the bait
- Catches of the month: A round-up of the latest phishing scams

With phishing, scammers don't need to monitor inboxes and send tailored responses. They simply dump thousands of crafted messages on unsuspecting people.

As such, there's no need to filter out potential respondents. Doing so reduces the pool of potential victims and helps those who didn't fall victim to alert others to the scam, as we saw in the earlier example with Gimlet Media.

So why are many phishing emails poorly written? In this case, the most obvious answer is the correct one: the scammers aren't very good at writing.

Remember, many of them are from non-English-speaking countries and backgrounds where they will have limited access or opportunity to learn the language.

With this in mind, it becomes much easier to spot the difference between a typo made by a legitimate sender and a scam.

When crafting phishing messages, scammers often use a spellchecker or translation machine, giving them all the right words but not necessarily in the proper context.

Take this example of a scam imitating Windows:

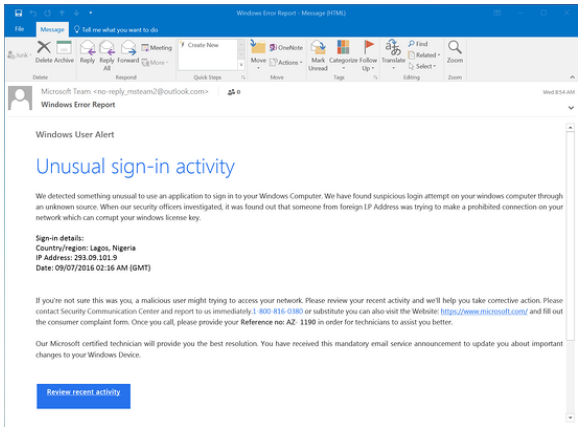


Image: KnowBe4
No individual word is misspelt, but the message contains grammatical errors that a native speaker wouldn't make, such as "We detected something unusual to use an application".

Likewise, there are strings of missed words, such as "a malicious user might trying to access" and "Please contact Security Communication Center".

These are consistent with the kinds of mistakes people make when learning English. Any supposedly official message written this way is almost certainly a scam.

That's not to say any email with a mistake is a scam, however. Everyone makes typos from time to time, especially when they're in a hurry.

It's, therefore, the recipient's responsibility to look at the context of the error and determine whether it's a clue to something more sinister. You can do this by asking:

- *Is it a common sign of a typo (like hitting an adjacent key)?*
- *Is it a mistake a native speaker shouldn't make (grammatical incoherence, words used in the wrong context)?*
- *Is this email a template which should have been crafted and copy-edited?*
- *Is it consistent with previous messages I've received from this person?*

If you're in any doubt, look for other clues that we've listed here or contact the sender using another line of communication, whether in person, by phone, via their website, an alternative email address or through an instant message client.

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.

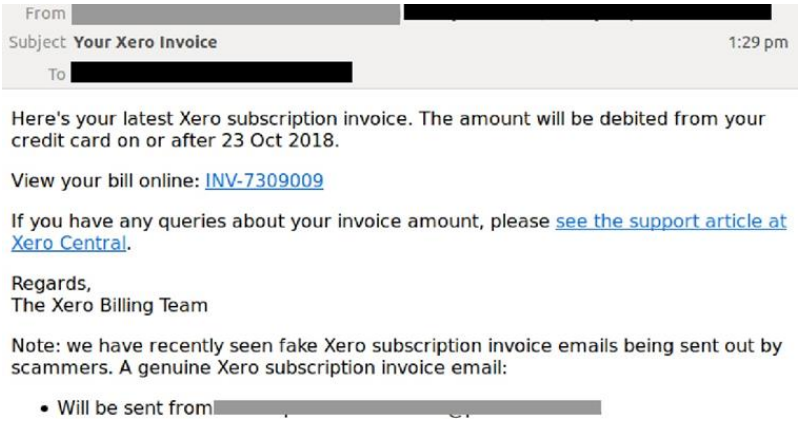
But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment you're asked to download or a link to a bogus website.

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

In this next section, we'll explain how each of those works.

Infected attachments

An infected attachment is a seemingly benign document that contains malware.
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]

It doesn't matter whether the recipient expects to receive an invoice from this person or not because, in most cases, they won't be sure what the message pertains to until they open the attachment.

When they open the attachment, they'll see that the invoice isn't intended for them, but it will be too late. The document unleashes malware on the victim's computer, which could perform any number of nefarious activities. We advise that you never open an attachment unless you are confident that the message is from a legitimate party. Even then, you should look out for anything suspicious in the attachment.

For example, if you receive a pop-up warning about the file's legitimacy or the application asks you to adjust your settings, then don't proceed.

Suspicious links

You can spot a suspicious link if the destination address doesn't match the context of the rest of the email.

For example, if you receive an email from Netflix, you would expect the link to direct you towards an address that begins 'netflix.com'.

Unfortunately, many legitimate and scam emails hide the destination address in a button, so it's not immediately apparent where the link goes.

n this example, the scammers are claiming that there is an issue with the recipient's Netflix subscription. The email is designed to direct them to a mock-up of Netflix's website, where they will be prompted to enter their payment details.

The fraudsters achieve two things by including the link within a button that says 'Update account now'.

First, it makes the message look genuine, with buttons becoming increasingly popular in emails and websites. But more importantly, it hides the destination address, making it a hyperlink.

To ensure you don't fall for schemes like this, you must train yourself to check where links go before opening them.

Thankfully, this is straightforward: on a computer, hover your mouse over the link, and the destination address appears in a small bar along the bottom of the browser.

On a mobile device, hold down on the link, and a pop-up will appear containing the link.

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.

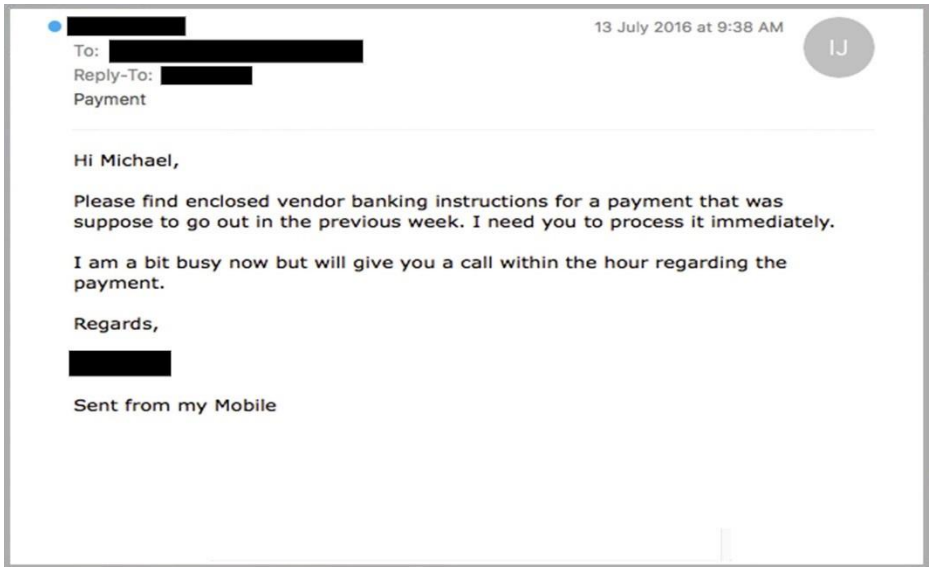
That's why so many scams request that you act now, or else it will be too late. This has been evident in every example we've used so far.

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.

Criminals know that we're likely to drop everything if our boss emails us with a vital request, especially when other senior colleagues are supposedly waiting on us.

A typical example looks like this:



Phishing scams like this are particularly dangerous because, even if the recipient did suspect foul play, they might be too afraid to confront their boss.

After all, if they are wrong, they're implying that there was something unprofessional about the boss's request.

However, organisations that value cyber security would accept that it's better to be safe than sorry and perhaps even congratulate the employee for their caution.

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.

*With our **Phishing Staff Awareness Training Programme**, these lessons are straightforward.*

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

Guidelines to be followed while accessing public systems :

- *Never pass or tell the Cyber Cafe Owner or anyone else about your email and password to check your e-mail.*

Fact : *surveys say that small kids or many old aged persons have no idea about the risks of information theft.*

- *If you store or download any personal information on Desktop in cyber cafe make sure you delete all the documents after you complete your work. Disable the option "Remember my ID on the computer" and use Strong Password.*

- *When surfing the Internet, you should always check the browser security like default download folder, cookies and password save locations etc., to avoid risks of exposing personal information. As a precaution use Incognito Mode of the browser to avoid storing your personal details in the cookies.*

- *A keylogger is basically spyware, it logs or records your keystrokes so that your username and password are made available to Cyber cafe owner or any Attacker. The records you enter maybe typed directly into Hacker's machine or collected afterwards through a file transfer.Always check if there is an intermediate device between your keyboard and CPU. Where ever possible, prefer using on screen keyboards.*

- *Ensure that that the system you are using has most up-to-date Anti Virus and Anti spam software. These may help to stop some of the key loggers, Trojans and other malware. You can insist cyber cafe Owner to allocate you a computer loaded with updated antivirus software.*

- *Do not leave the computer unattended with sensitive information on the screen. Remember to check Downloads folder for automatically saved files.*

- *Do not enter sensitive information into a public computer.*

- *Look for camera facing your keyboard to monitor your key strokes. There can be hidden cameras also for such shoulder surfing. Be cautious.*

ew 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.*

-Subscribe to the selected channels

You may also subscribe to specific selected channels by selecting subscribe button. This will ensure that you will be directed to the specific videos that you want to watch.

For subscribing to selected channels

- *open the youtube app or goto youtube.com*
- *sign in with your credentials*
- *select the type of videos you want to view*
- *select the subscribe button.*

-Enable restricted mode on youtube

Youtube provides the 'Restricted Mode' on regular youTube website, which will enable a kid-friendly setting, with restricted content. Parents may use the same for older children, to avoid inappropriate content.

To set up YouTube Restricted Mode

- *go to YouTube.com and sign into the account you created*
- *Scroll down to the very bottom of the page.*
- *Then click Restricted Mode.*
- *You will see some safety buttons appear below.*
- *Click the circle labelled "On," to enable Restricted Mode.*
- *Then click Save to save the changes you've made to your settings.*

-Upload videos by selecting private or unlisted option and restrict comments

For a safe video sharing option you may guide the child to upload viedo privately to selected members, you may use the unlisted option so that they do not show up on youtube option but anyone with specific link can only see it, you can also restrict comments from viewers, to avoid disturbing reviews.

To enable this option signin to youtube studio, from left menu select videos, hover over the video you want to update, click down arrow under visibility and choose private or unlisted option and save.

(reference: https://techboomers.com/youtube-parental-controls)

- ***Enable parental controls for activating security features and safeguarding children***

Parental controls are restrictions that parents can implement on child's usage of digital devices by enabling certain features available in the software of specific devices and monitor their online activity. It helps reduce the risk of child viewing inappropriate content on web.

The parental control can help

- *Block inappropriate apps., games and media child can access*
- *Set restrictions on web browsers to show only pre-approved websites*
- *Restrict search engines by defining what child can search online*
- *Restrict child from using certain unwanted services*

Steps to set up parental controls:

- *Open google play store app*
- *Tap menu in the top right corner*
- *Got to settings*
- *Go to parental controls option and turn it on*
- *Create a PIN*
- *Tap the type of content you want to filter*
- *Choose how to filter or restrict access.*

Other options to monitor online activities of children

- *Parents may **use security features enabled parental control/ child monitoring apps**, available on google playstore to help them in guiding children appropriately on digital device usage and safeguard them against possible online dangers.*

Examples of few parental control Apps – Net Nanny, Norton Family, Kasperskey safe kids, Bark, mspy etc.,

- *Have digital device usage family agreements, where all the family agree to follow certain common family rules for using digital devices.*
- *Have digital free zones like bedtime, dinner time, play time, driving time etc.,*
- *Model kindness and good digital usage habits, when using digital medium for communication.*

- ***Be a good Digital Role Model***

  Modeling good digital habits is essential for parents. This is important as the parents behavior and habits are unspoken permission to children to practice the same later on.

  - *Do not engage too much in digital devices when you are around children.*
  - *Pay attention to children and to what they want to tell you.*
  - *Engage in positive, encouraging and motivating approach while talking to children*
  - *Create an environment wherein children can put across their digital issues, to parents to seek suggestions.*
  - *Help children to form confident ideas and beliefs about themselves to deal with crisis situations.*
  - *Be accessible to children; have certain time in a day allocated to family and children*

Guidelines to be followed while accessing public systems :

- *Never pass or tell the Cyber Cafe Owner or anyone else about your email and password to check your e-mail.*

Fact : *surveys say that small kids or many old aged persons have no idea about the risks of information theft.*

- *If you store or download any personal information on Desktop in cyber cafe make sure you delete all the documents after you complete your work. Disable the option "Remember my ID on the computer" and use Strong Password.*

- *When surfing the Internet, you should always check the browser security like default download folder, cookies and password save locations etc., to avoid risks of exposing personal information. As a precaution use Incognito Mode of the browser to avoid storing your personal details in the cookies.*

- *A keylogger is basically spyware, it logs or records your keystrokes so that your username and password are made available to Cyber cafe owner or any Attacker. The records you enter maybe typed directly into Hacker's machine or collected afterwards through a file transfer.Always check if there is an intermediate device between your keyboard and CPU. Where ever possible, prefer using on screen keyboards.*

- *Ensure that that the system you are using has most up-to-date Anti Virus and Anti spam software. These may help to stop some of the key loggers, Trojans and other malware. You can insist cyber cafe Owner to allocate you a computer loaded with updated antivirus software.*

- *Do not leave the computer unattended with sensitive information on the screen. Remember to check Downloads folder for automatically saved files.*

- *Do not enter sensitive information into a public computer.*

- *Look for camera facing your keyboard to monitor your key strokes. There can be hidden cameras also for such shoulder surfing. Be cautious.*

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

This document describes the information to help you secure your Cisco IOS• system devices, which increases the overall security of your network. Structured around the three planes into which functions of a network device can be categorized, this document provides an overview of each included feature and references to related documentation.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The three functional planes of a network, the management plane, control plane, and data plane, each provide different functionality that needs to be protected.

- **Management Plane** - The management plane manages traffic that is sent to the Cisco IOS device and is made up of applications and protocols such as Secure Shell (SSH) and Simple Network Management Protocol (SNMP).

- **Control Plane** - The control plane of a network device processes the traffic that is paramount to maintain the functionality of the network infrastructure. The control plane consists of applications and protocols between network devices, which includes the Border Gateway Protocol (BGP), as well as the Interior Gateway Protocols (IGPs) such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF).

- **Data Plane** - The data plane forwards data through a network device. The data plane does not include traffic that is sent to the local Cisco IOS device.

The coverage of security features in this document often provides enough detail for you to configure the feature. However, in cases where it does not, the feature is explained in such a way that you can evaluate whether additional attention to the feature is required. Where possible and appropriate, this document contains recommendations that, if implemented, help secure a network.

Secure Operations

Secure network operations is a substantial topic. Although most of this document is devoted to the secure configuration of a Cisco IOS device, configurations alone do not completely secure a network. The operational procedures in use on the network contribute as much to security as the configuration of the underlying devices.

These topics contain operational recommendations that you are advised to implement. These topics highlight specific critical areas of network operations and are not comprehensive.

Monitor Cisco Security Advisories and Responses

The Cisco Product Security Incident Response Team (PSIRT) creates and maintains publications, commonly referred to as PSIRT Advisories, for security-related issues in Cisco products. The method used for communication of less severe issues is the Cisco Security Response. Security advisories and responses are available at http://www.cisco.com/go/psirt.
Additional information about these communication vehicles is available in the Cisco Security Vulnerability Policy.
In order to maintain a secure network, you need to be aware of the Cisco security advisories and responses that have been released. You need to have knowledge of a vulnerability before the threat it can pose to a network can be evaluated. Refer to Risk Triage for Security Vulnerability Announcements for assistance this evaluation process.

Leverage Authentication, Authorization, and Accounting

The Authentication, Authorization, and Accounting (AAA) framework is vital to secure network devices. The AAA framework provides authentication of management sessions and can also limit users to specific, administrator-defined commands and log all commands entered by all users. See the Authentication, Authorization, and Accounting section of this document for more information about how to leverage AAA.

Centralize Log Collection and Monitoring

In order to gain knowledge about existing, emerging, and historic events related to security incidents, your organization must have a unified strategy for event logging and correlation. This strategy must leverage logging from all network devices and use pre-packaged and customizable correlation capabilities.

After centralized logging is implemented, you must develop a structured approach to log analysis and incident tracking. Based on the needs of your organization, this approach can range from a simple diligent review of log data to advanced rule-based analysis.

See the Logging Best Practices section of this document for more information about how to implement logging on Cisco IOS network devices.

Use Secure Protocols When Possible

Many protocols are used in order to carry sensitive network management data. You must use secure protocols whenever possible. A secure protocol choice includes the use of SSH instead of Telnet so that both authentication data and management information are encrypted. In addition, you must use secure file transfer protocols when you copy configuration data. An example is the use of the Secure Copy Protocol (SCP) in place of FTP or TFTP.

See the Secure Interactive Management Sessions section of this document for more information about the secure management of Cisco IOS devices.

Gain Traffic Visibility with NetFlow

NetFlow enables you to monitor traffic flows in the network. Originally intended to export traffic information to network management applications, NetFlow can also be used in order to show flow information on a router. This capability allows you to see what traffic traverses the network in real time. Regardless of whether flow information is exported to a remote collector, you are advised to configure network devices for NetFlow so that it can be used reactively if needed.

More information about this feature is available in the Traffic Identification and Traceback section of this document and at http://www.cisco.com/go/netflow (registered customers only) .

Configuration Management

Configuration management is a process by which configuration changes are proposed, reviewed, approved, and deployed. Within the context of a Cisco IOS device configuration, two additional aspects of configuration management are critical: configuration archival and security.

You can use configuration archives to roll back changes that are made to network devices. In a security context, configuration archives can also be used in order to determine which security changes were made and when these changes occurred. In conjunction with AAA log data, this information can assist in the security auditing of network devices.

The configuration of a Cisco IOS device contains many sensitive details. Usernames, passwords, and the contents of access control lists are examples of this type of information. The repository that you use in order to archive Cisco IOS device configurations needs to be secured. Insecure access to this information can undermine the security of the entire network.

Management Plane

The management plane consists of functions that achieve the management goals of the network. This includes interactive management sessions that use SSH, as well as statistics-gathering with SNMP or NetFlow. When you consider the security of a network device, it is critical that the management plane be protected. If a security incident is able to undermine the functions of the management plane, it can be impossible for you to recover or stabilize the network.

These sections of this document detail the security features and configurations available in Cisco IOS software that help fortify the management plane.

General Management Plane Hardening

The management plane is used in order to access, configure, and manage a device, as well as monitor its operations and the network on which it is deployed. The management plane is the plane that receives and sends traffic for operations of these functions. You must secure both the management plane and control plane of a device, because operations of the control plane directly affect operations of the management plane. This list of protocols is used by the management plane:

- Simple Network Management Protocol
- Telnet
- Secure Shell Protocol
- File Transfer Protocol
- HyperText Transfer Protocol / Secure HyperText Transfer Protocol
- Trivial File Transfer Protocol
- Secure Copy Protocol
- TACACS+
- RADIUS
- NetFlow
- Network Time Protocol
- Syslog

Steps must be taken to ensure the survival of the management and control planes during security incidents. If one of these planes is successfully exploited, all planes can be compromised.

Password Management

Passwords control access to resources or devices. This is accomplished through the definition a password or secret that is used in order to authenticate requests. When a request is received for access to a resource or device, the request is challenged for verification of the password and identity, and access can be granted, denied, or limited based on the result. As a security best practice, passwords must be managed with a TACACS+ or RADIUS authentication server. However, note that a locally configured password for privileged access is still needed in the event of failure of the TACACS+ or RADIUS services. A device can also have other password information present within its configuration, such as an NTP key, SNMP community string, or Routing Protocol key.

*The **enable secret** command is used in order to set the password that grants privileged administrative access to the Cisco IOS system. The **enable secret** command must be used, rather than the older **enable password** command. The **enable password** command uses a weak encryption algorithm.*

If no enable secret is set and a password is configured for the console tty line, the console password can be used in order to receive privileged access, even from a remote virtual tty (vty) session. This action is almost certainly unwanted and is another reason to ensure configuration of an enable secret.

*The **service password-encryption** global configuration command directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. Such encryption is useful in order to prevent casual observers from reading passwords, such as when they look at the screen over the muster of an administrator. However, the algorithm used by the **service password-encryption** command is a simple Vigen re cipher. The algorithm is not designed to protect configuration files against serious analysis by even slightly sophisticated attackers and must not be used for this purpose. Any Cisco IOS configuration file that contains encrypted passwords must be treated with the same care that is used for a cleartext list of those same passwords.*

*While this weak encryption algorithm is not used by the **enable secret** command, it is used by the **enable password** global configuration command, as well as the **password** line configuration command. Passwords of this type must be eliminated and the **enable secret** command or the Enhanced Password Security feature needs to be used.*

*The **enable secret** command and the Enhanced Password Security feature use Message Digest 5 (MD5) for password hashing. This algorithm has had considerable public review and is not known to be reversible. However, the algorithm is subject to dictionary attacks. In a dictionary attack, an attacker tries every word in a dictionary or other list of candidate passwords in order to find a match. Therefore, configuration files must be securely stored and only shared with trusted individuals.*