everest®

We underwrite opportunity.™

Cybersecurity

Identifying and avoiding Phishing in working environments

What is Phishing?

Phishing is **any malicious message** created to "Phish" a victim and steal their information and important personal data like credit card numbers, ID numbers or even access credentials.

Through which channels does Phishing typically happen?

- **Email**
- **SMS**
- **Social networks**
- **Phone**

The attackers' greatest rule is to create a sophisticated and convincing message imitating, for example, your business contacts or friends.

Why is so dangerous from a company point of view?

- It can cause an organization **considerable financial loss.**
- It can permanently **damage the organization's reputation** with partners, clients, and business associates.

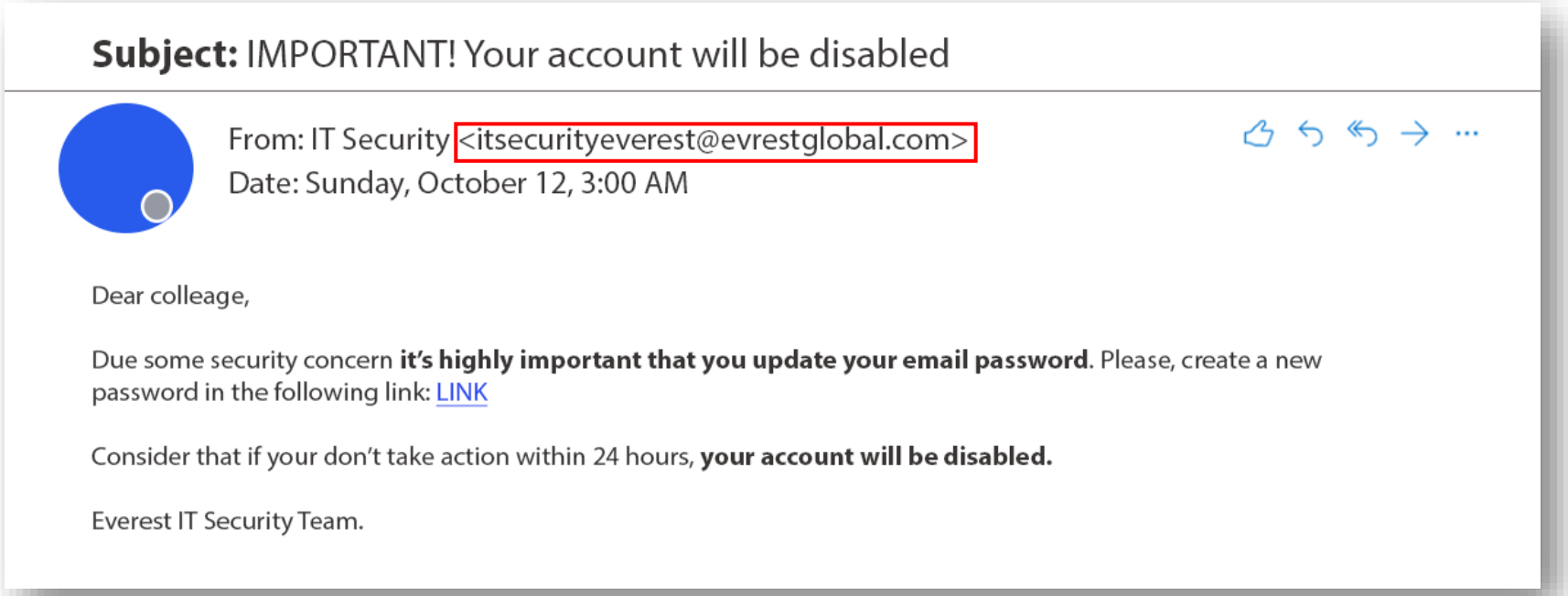
Why is so dangerous from a personal point of view?

- It can **steal your identity** and use it to commit fraud.
- It can put your **family and friends at risk** since they might receive fake emails or messages from you.

Easy recognizable signals of Phishing

- From

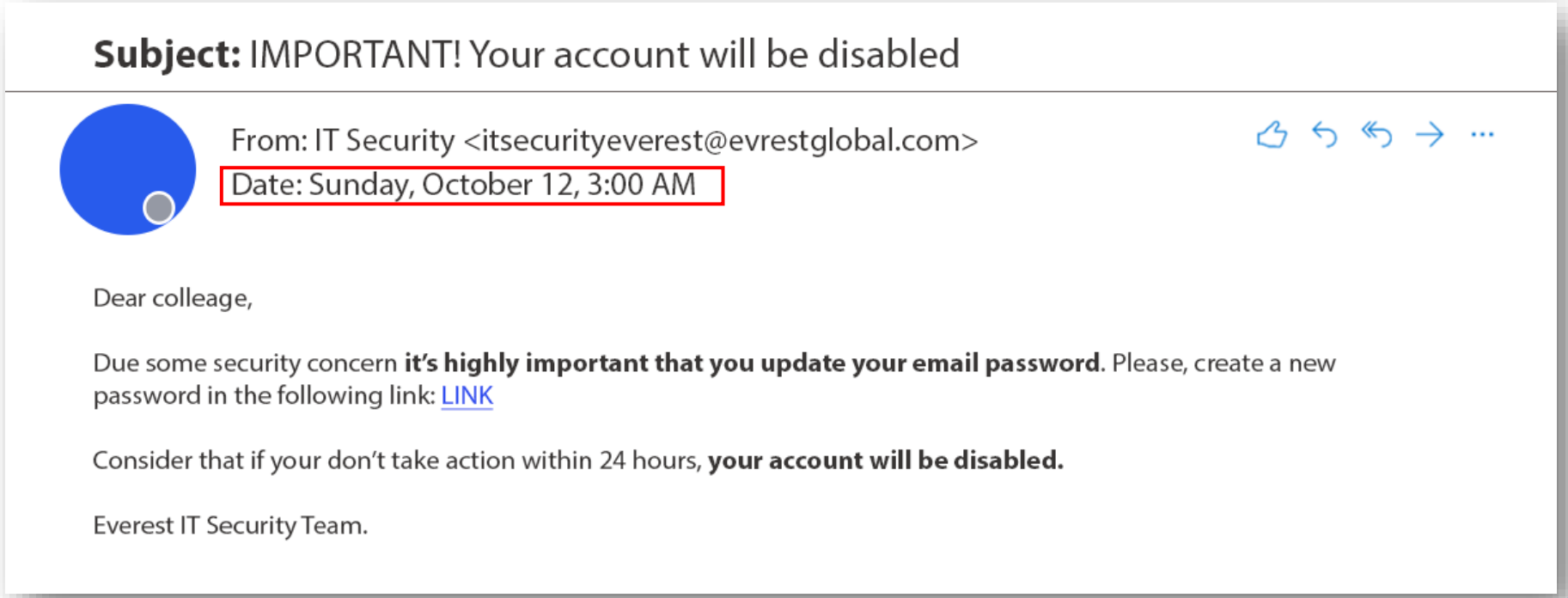
Look out for **addresses from people you don't know or weren't expecting, spelling errors, or addresses that look slightly out of the ordinary.** Cybercriminals often impersonate people you know by using lookalike email addresses. Use your bookmarked sites or a phone number you know is legitimate to verify the request from the true source.



Easy recognizable signals of Phishing

- Date

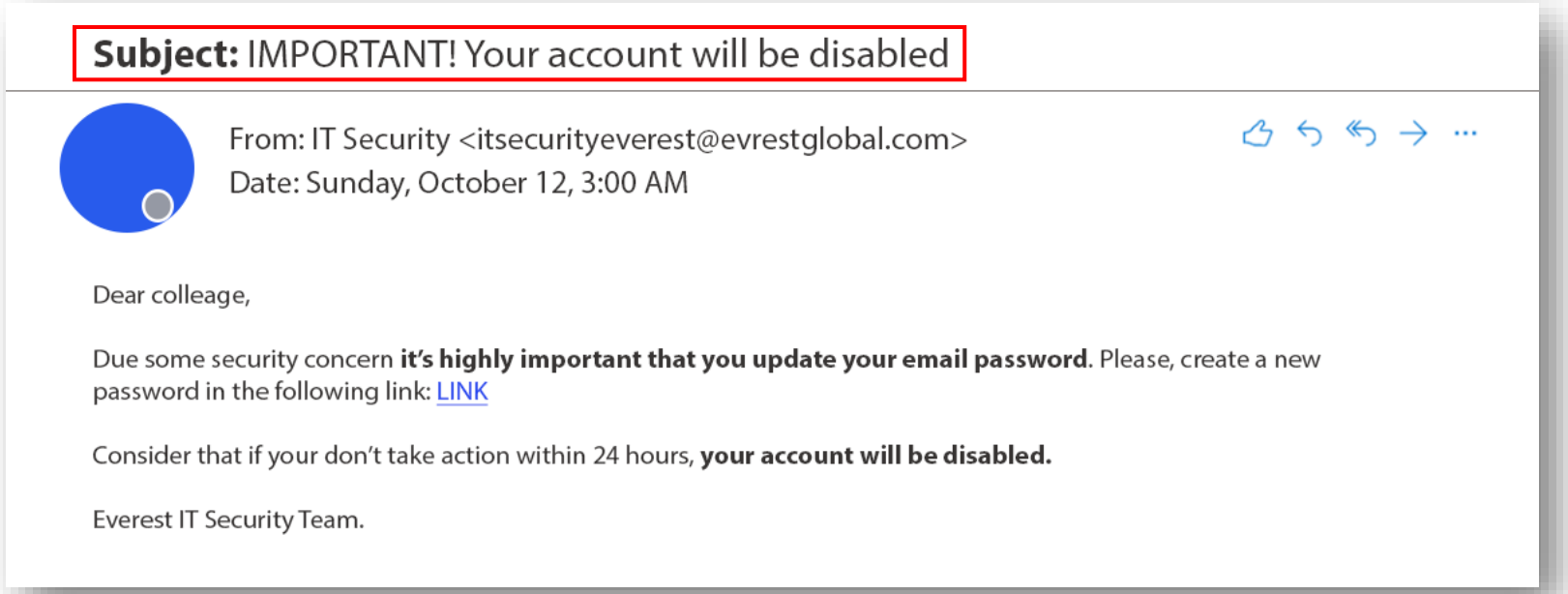
Messages sent at irregular hours should raise a red flag. A message sent at 3:00 a.m. for example, or even message sent during the weekends.



Easy recognizable signals of Phishing

- Subject

Cybercriminals will use the subject line to **pique your attention and draw you into interacting** with the rest of the email. Check the subject line matches that of the content. Is it a reply to something you didn't request? Is it a forwarded message that doesn't apply to you? Were you expecting this message? Does the request align with your company regular duct?

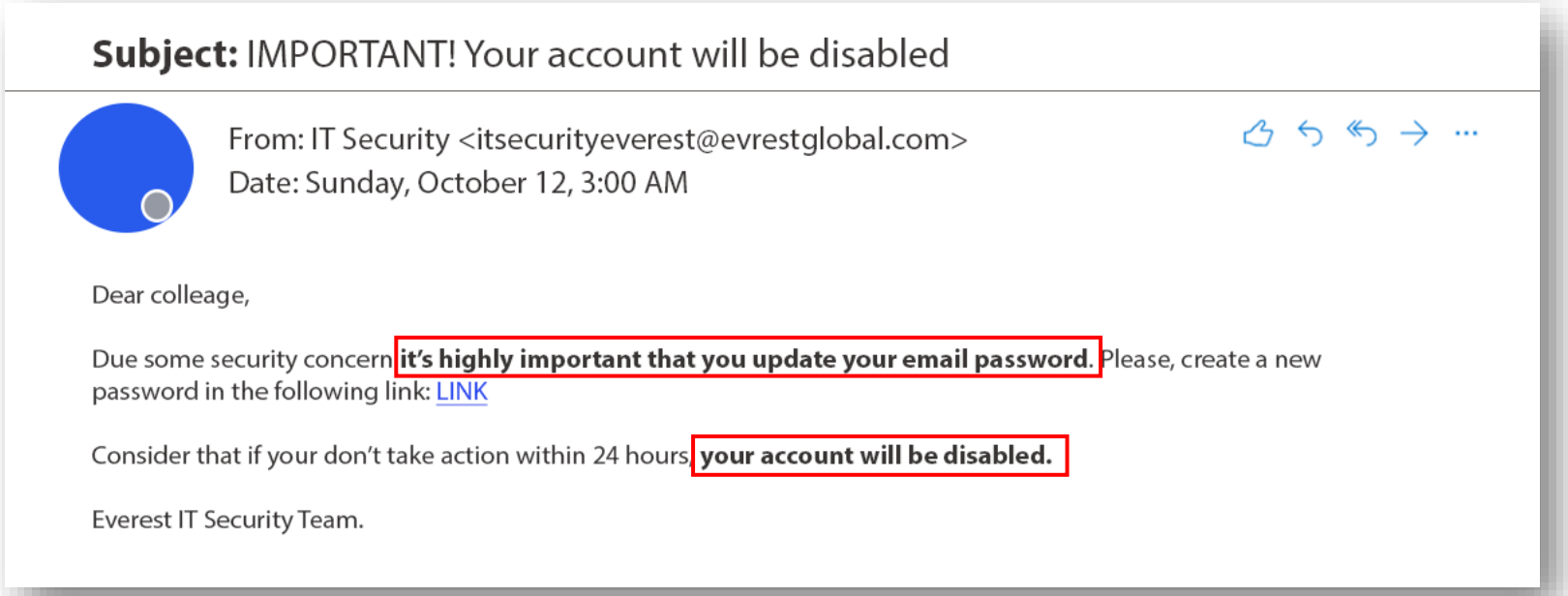


Easy recognizable signals of Phishing

- Sense of urgency

Phishing emails often **create a false sense of urgency to pressure you** into taking immediate action. For example: "If you don't act within 24 hours, your account will be disabled" or "As a security measure, we will delete your account if you don't respond within the next 24 hours.

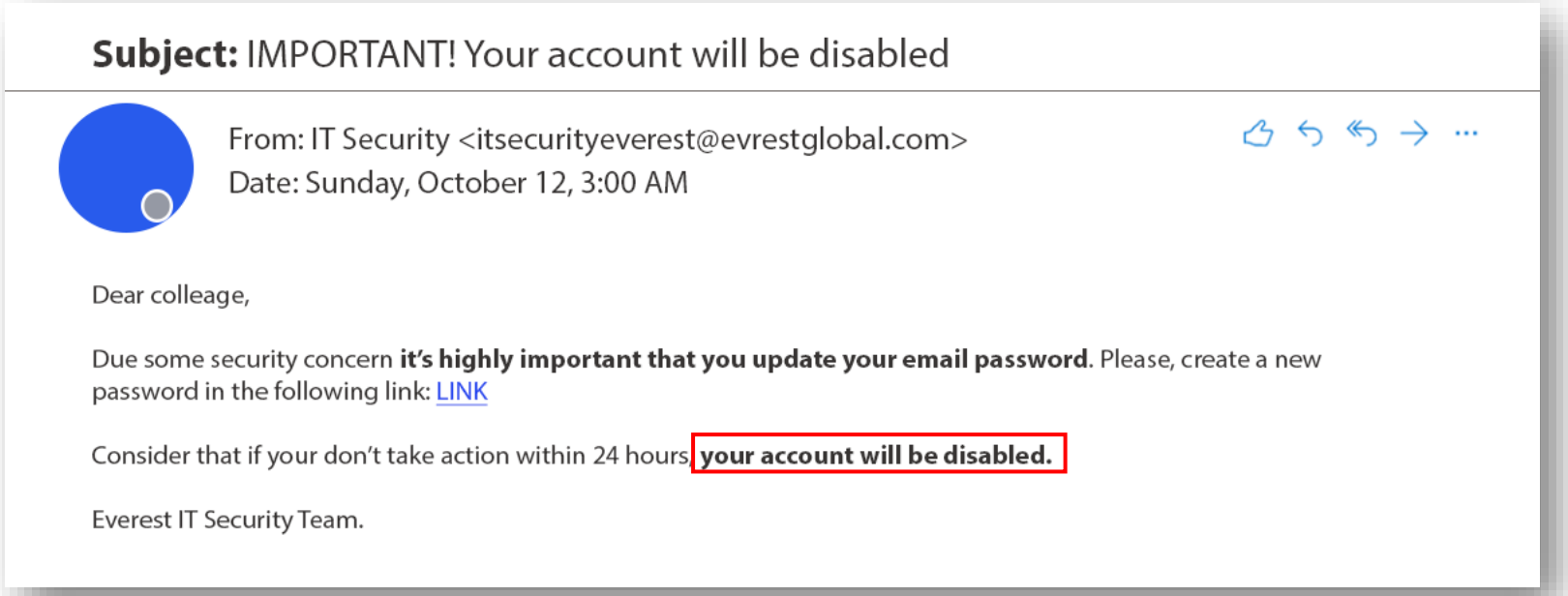
Keep in mind: legitimate companies, including yours, will never give such short deadlines to verify your account, update your password, or perform similar actions.



Easy recognizable signals of Phishing

- Fear or negative consequences

Another common tactic in Phishing emails is to create a sense of fear in the recipient. These messages may include **threats or warnings of negative consequences to pressure the user** into taking immediate action. Attackers often use basic personal information—easily found online—to make the message feel more targeted and convincing. If you copy and paste the entire email into a search engine such as Google, you'll notice other users had reported it as a scam.

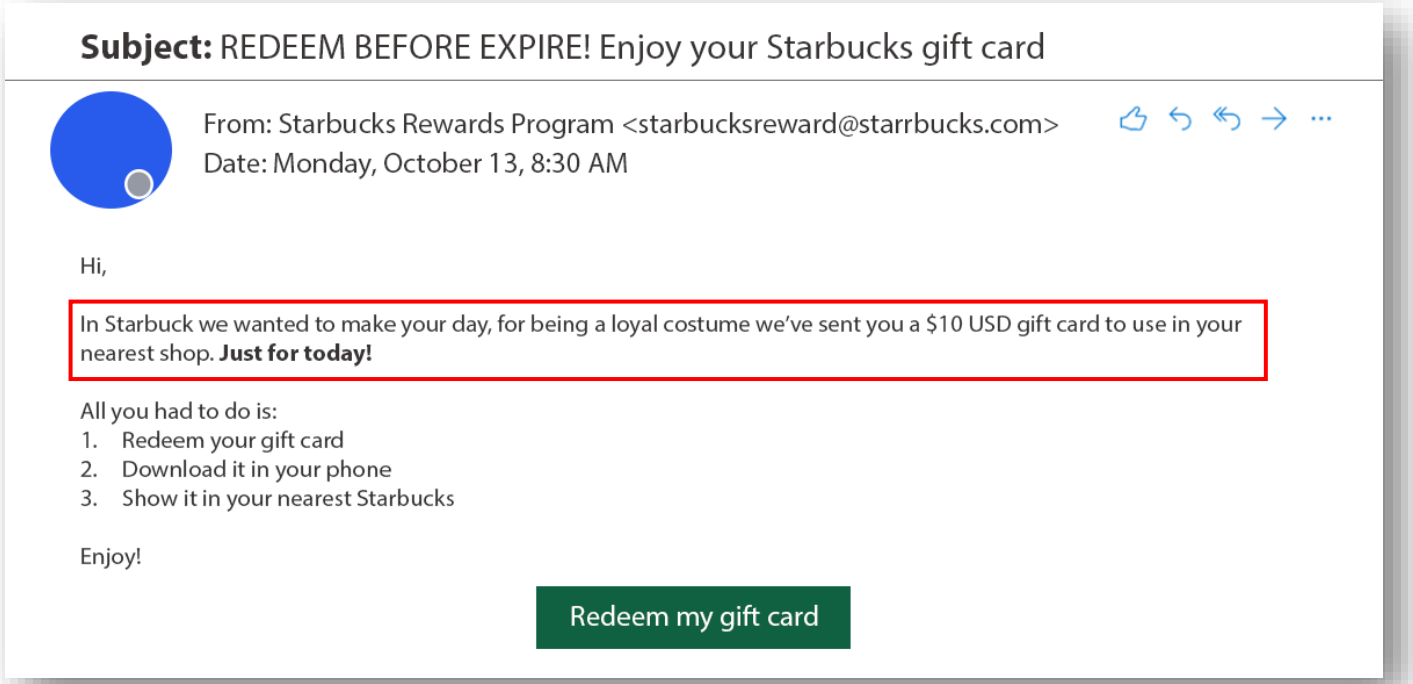


Easy recognizable signals of Phishing

- Promises of gifts or rewards

Many Phishing attempts involve **false offers such as gift cards, prizes, or exclusive deals** to lure you into clicking on malicious links.

Do not trust unexpected emails offering rewards. Remember, if it sounds too good to be true, it probably is.



How do you know if a link is malicious?

First, **hover your mouse over the link so you can see the complete URL** before clicking and judge it.

How to judge it? To understand what you're seeing, let's break down the structure of a URL (specifically what comes before and after the main domain)

- **Subdomain:** is what comes before the main domain name, separated by a dot. Common examples include:
  - **www** → www.everestglobal.com
  - **mail** → mail.everestglobal.com
  - **blog** → blog.everestglobal.com
  - **store** → store.everestglobal.com

  These are used to organize different parts of a website. They can be real, but attackers may fake them to mislead you. Just because you see "paypal" in a subdomain like paypal.site.com doesn't mean it's a real paypal site.
- **TLD (Top-Level Domain) :** is what comes after the main domain name. Examples include:
  - **.com** → www.everestglobal.com
  - **.org** → www.everestglobal.org
  - **.net** → www.everestglobal.net
  - **.edu** → www.everestglobal.edu

Examples

Subdomain

- **https://safety.everestglobal.com**

  In this case ‘safety’ is separated from the primary domain by a period which makes ‘safety’ a **subdomain**. This mean you should be able to trust the site, since the main domain is everestglobal.com

Sub-directories

- **https://everestglobal.com/safety/main**

  In this case ‘safety’ and ‘main’ are separated by the forward slashes and they become **sub-directories** of the original site of Everest.

Main domain

- **https://everestglobal.safety.com**

  In this case safety.com would become the **main domain** and by clicking on the link you would be redirected to that website and not to everestglobal.com. Be cautious!

What are some other signs of malicious or fakes links?

- **Periods:** periods that split the domain name can totally change the main domain, for example, in this case we will be directed to 'global.com':
  - https://everest.global.com
- **Hyphen:** a hyphen in the domain name changes the actual domain. It becomes part of the main domain, not just an extra word. In this case you're visiting a site called 'secure-everestglobal.com' that has nothing to do with 'everestglobal.com':
  - https://secure-everestglobal.com
- **Numbers:** numbers before a domain are suspicious, as they may indicate a potential security risk, like Phishing. However, if numbers appears after a domain, they can represent content identifiers, page numbers, or query parameters. So, only when you see numbers *before* the main domain, do not trust:
  - 192.45.34.72.everestglobal.com
- **Shortened URL:** a shortened URL hides the real destination, making it easy to disguise malicious sites and trick people into clicking without knowing the real target site, always double check before clicking:
  - https://bit.ly/49Pd3MK
- **Spelling errors:** subtle spelling errors will mislead you into thinking that they are the legitimate site. Always give an extra look at the URL before clicking
  - https://evrestglobal.com

Tips to avoid a Phishing attempt

To check if a link is real, manually type the URL into a search engine such as Google. Search for the exact URL along with words like “review”, “scam” or “fake”. The results should make it clear whether the link is legitimate or a Phishing attempt.

If someone you know sends a file you weren’t expecting, verify it was really them, using a contact method you know is legitimate. Do not download or run unsolicited files.

Avoid accessing your email or social media accounts on public computers or open Wi-Fi Networks. These environments are often not secure, and attackers can intercept your personal data more easily, especially if the connection is unencrypted.

everest®

We underwrite opportunity.™

Thank you for completing this course.