**What is Phishing vs Spear Phishing?**

Organizations have sensitive data that cybercriminals are always on the lookout for. It can be data pertaining to the business itself, or customer data including their personal, financial or health information. Just as technology is advancing every passing day, so are the techniques used by hackers to get access to confidential information.

**What is Phishing?**

One such technique is called a phishing scam, which is a fake message usually sent by an email, and tricks you into giving your personal or financial information. The sender impersonates as an individual or company you know or trust, and asks you to click a link, download an attachment, fill a form or simply give out your information. The messages are designed to look real, with same company logos, similar email addresses and links to authentic-looking websites. Besides email, phishing messages are also sent via text messages and social media platforms. With the help of phishing scams, hackers intend to steal your confidential information such as credit card details, online banking logins, business logins, passwords and other personal data. It can affect anyone, from an individual internet user to an employee of a company.

This trend has also increased after the spread of Coronavirus where criminals are using emails, text messages and websites that impersonate official Australian and international organizations such as Health Department or World Health Organization. They claim to give official information about the pandemic, but actually intend to get your information.

**How to Detect a Phishing Scam?**

Even though phishing messages are mostly professionally designed and hard to detect, there are still some signs which can help you identify them.

* If the email is from an individual you know, check their email address to confirm if the message came from the same address or a different one
* Always check the domain name of the email address, for instance, @knowncompany.com.au. If the domain is same as the original website domain of the company or brand, the email is probably not fake. If the domain of email address is slightly different, it is a sign of scam. Criminals often use domain names that are similar to the original website domain.
* If a message is asking you to open an unknown attachment, link or picture, check it for authenticity before opening it. You can do it in a number of ways:
  + Hover your cursor over the link name or attachment to see where it redirects you – if the link looks suspicious to you, don’t click it
  + Call the organization or individual by getting their contact details from a reliable source and not the one mentioned in the message. Ask them to verify the contents of the email
* Don’t respond if an email has poor grammar or spelling errors
* If an email is offering a deal that seems too good to be true, it is probably fake. E.g. “Earn $3000 everyday by doing nothing”, “You have won a lottery worth $1M”, and similar messages.
* A message from a financial institution or your bank, asking you to fill your credit card or online account password details is highly suspicious as banks never ask for confidential information through emails.
* Messages that claim to be from a government department or an established business but sent from generic email addresses such as Gmail or Hotmail indicate malicious intent

**Phishing vs Spear Phishing**

Spear Phishing is a variant of Phishing, where the hacker targets a specific victim for malicious reasons. Whereas phishing attacks are random and can be targeted at anyone in general, spear phishing attacks are planned to directly aim a known victim. This is done by getting their personal details, such as employer, hometown, friends and frequently-visited locations. The criminals then use this information to their advantage and create legitimate-looking messages to trap the victim. Because of their personalized nature, spear phishing emails are more likely to succeed as compared to generic phishing messages. In fact, according to a report, spear phishing is the most successful way of accessing private information online, and accounts to [91 percent](https://www.firmex.com/resources/infographics/spear-phishing-whos-getting-caught/) of attacks on the internet.

**How Spear Phishing Emails Work?**

Spear phishing emails are not easy to detect without past knowledge about spear phishing protection. The victims of these attacks are mostly individuals who put their personal information on the internet, mainly on social networking websites. They can then identify that person’s email address, friends, geographical location and other important details, and send a convincing fraudulent message according to the victim’s profile.

To ensure the success of spear phishing emails, the messages usually demand urgency on why they require sensitive information. When the victim opens a malicious link, it directs them to a spoofed website which asks for passwords, PINs, account number or access codes. Once they gather the information, they can access the victim’s bank account or even create a fake identity in their name.

**How to Avoid a Spear Phishing Attack?**

Whether as an individual or an employee, you should never respond to any unknown messages that request for personal information or ask to click suspicious links, as it can lead to a serious personal or business email compromise. Here are some precautions businesses must teach their employees to prevent them from being victims of spear phishing attacks:

* Examine your personal information that you have posted on the internet. Do not post too many details about yourself, and don’t put anything you would not want a potential scammer to see. Limit your privacy settings.
* Don’t use the same password for all accounts so if a hacker finds out the password to one of your accounts, they are unable to access others. Follow [best practices](https://krebsonsecurity.com/password-dos-and-donts/) for keeping strong passwords.
* Update your software frequently as software updates provide vulnerability patches to help protect you against common attacks. Enable automatic updates where possible.
* Never open a link in Email right away. Always ensure the legitimacy of the email first and then open the link. Also examine the link by hovering your mouse over it before opening it.
* If you get a message from a “friend” asking you for sensitive information, verify it from them through another medium such as telephone.
* Practice safe online behavior by following best practices for [email](https://www.cyber.gov.au/node/1522) and [internet browsing](https://www.cyber.gov.au/node/1520).
* Keep yourself informed of the [latest threats](https://www.cyber.gov.au/node/1601/) and trending [scams](https://www.scamwatch.gov.au/)
* Most importantly, implement a data security solution at your organization for conforming to best practices and security from phishing threats

**KMTech’s Cyber Assessment Solution**

Our vulnerability assessment solution is especially designed to help small and medium businesses deal proactively with emerging threats and prevent data breaches resulting from phishing and spear phishing attacks. We provide detailed assessment on your security loopholes and propose remedial solutions. Book your [free cybersecurity vulnerability assessment](https://kmtech.com.au/book-a-cyber-assessment/) with us today!