PHISHING ANALYSIS-

Phishing analysis links-

<https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full>

### Real-World Phishing Examples

Some real-world examples of phishing attacks are discussed in this section to present the complexity of some recent phishing attacks. [Figure 2](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#F2) shows the screenshot of a suspicious phishing email that passed a University’s spam filters and reached the recipient mailbox. As shown in [Figure 2](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#F2), the phisher uses the sense of importance or urgency in the subject through the word ‘important,’ so that the email can trigger a psychological reaction in the user to prompt them into clicking the button “View message.” The email contains a suspicious embedded button, indeed, when hovering over this embedded button, it does not match with Uniform Resource Locator (URL) in the status bar. Another clue in this example is that the sender's address is questionable and not known to the receiver. Clicking on the fake attachment button will result in either installation of a virus or worm onto the computer or handing over the user’s credentials by redirecting the victim onto a fake login page.

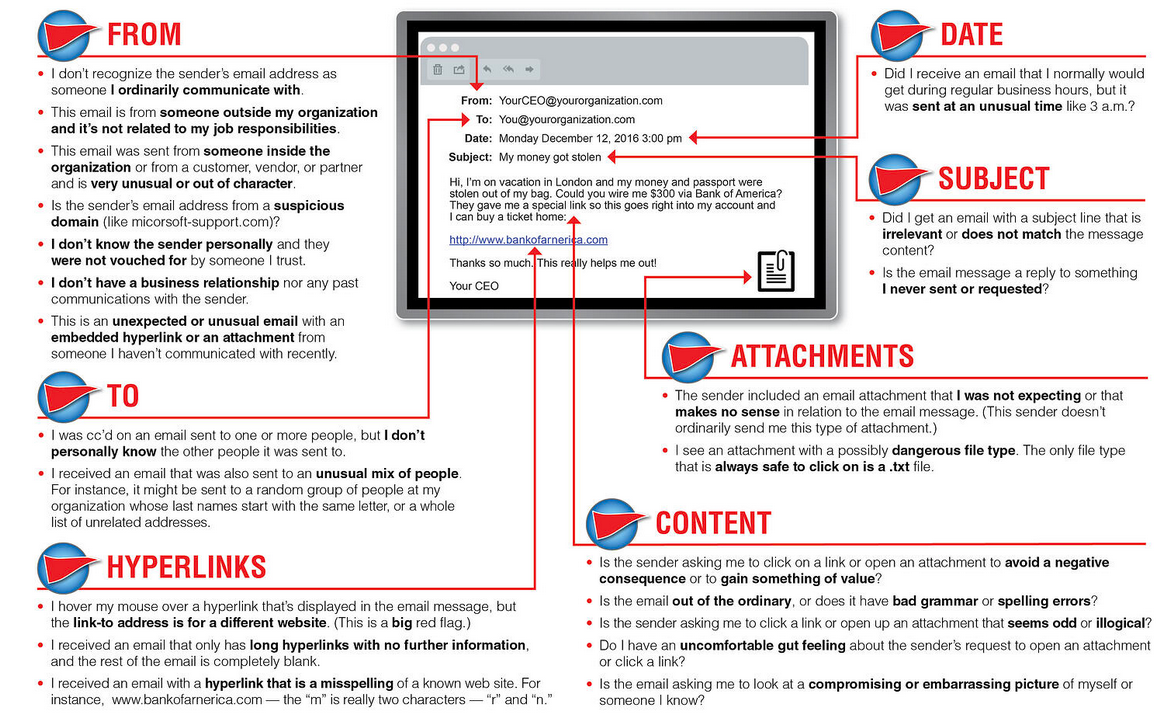
More recently, phishers take advantage of the Coronavirus pandemic (COVID-19) to fool their prey. Many Coronavirus-themed scam messages sent by attackers exploited people’s fear of contracting COVID-19 and urgency to look for information related to Coronavirus (e.g., some of these attacks are related to Personal Protective Equipment (PPE) such as facemasks), the WHO stated that COVID-19 has created an Infodemic which is favorable for phishers ([Hewage, 2020](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full" \l "B46)). Cybercriminals also lured people to open attachments claiming that it contains information about people with Coronavirus within the local area.

[Figure 3](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#F3) shows an example of a phishing e-mail where the attacker claimed to be the recipient’s neighbor sending a message in which they pretended to be dying from the virus and threatening to infect the victim unless a ransom was paid ([Ksepersky, 2020](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full" \l "B63)).

Another example is the phishing attack spotted by a security researcher at Akamai organization in January 2019. The attack attempted to use Google Translate to mask suspicious URLs, prefacing them with the legit-looking “[www.translate.google.com](http://www.translate.google.com)” address to dupe users into logging in ([Rhett, 2019](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#B101)). That attack followed with Phishing scams asking for Netflix payment detail for example, or embedded in promoted tweets that redirect users to genuine-looking PayPal login pages. Although the tricky/bogus page was very well designed in the latter case, the lack of a Hypertext Transfer Protocol Secure (HTTPS) lock and misspellings in the URL were key red flags (or giveaways) that this was actually a phishing attempt ([Keck, 2018](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#B57)). [Figure 4A](https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#F4) shows a screenshot of a phishing email received by the Federal Trade Commission (FTC). The email promotes the user to update his payment method by clicking on a link, pretending that Netflix is having a problem with the user's billing information

<https://www.tessian.com/blog/phishing-statistics-2020/>

<https://www.phishing.org/what-is-phishing>



<https://blog.cyble.com/2023/03/14/svb-collapse-triggers-heightened-cybersecurity-concerns/>

<https://cyberpyin.wordpress.com/phishing-email-analysis/>

<https://medium.com/@ERBATMAN/blue-team-labs-phishing-analysis-1641b42dd9c9>

Phishing tool links-

<https://www.securitynguyen.com/phishing-analysis-tools/>