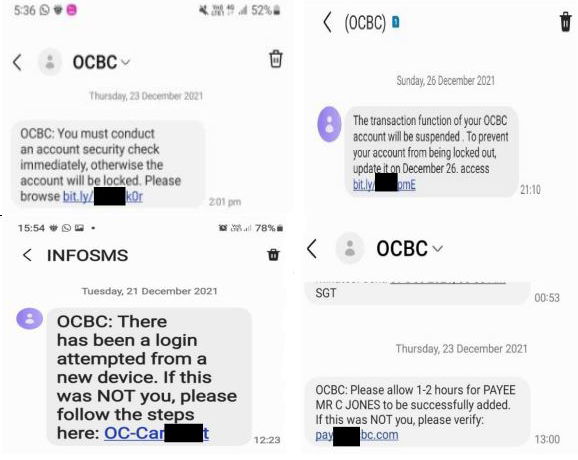
CSIRO Work Experience 2022- Cyber

**PHISHING CHARACTERISTICS**

AIMS and TACTICS

horizontal line

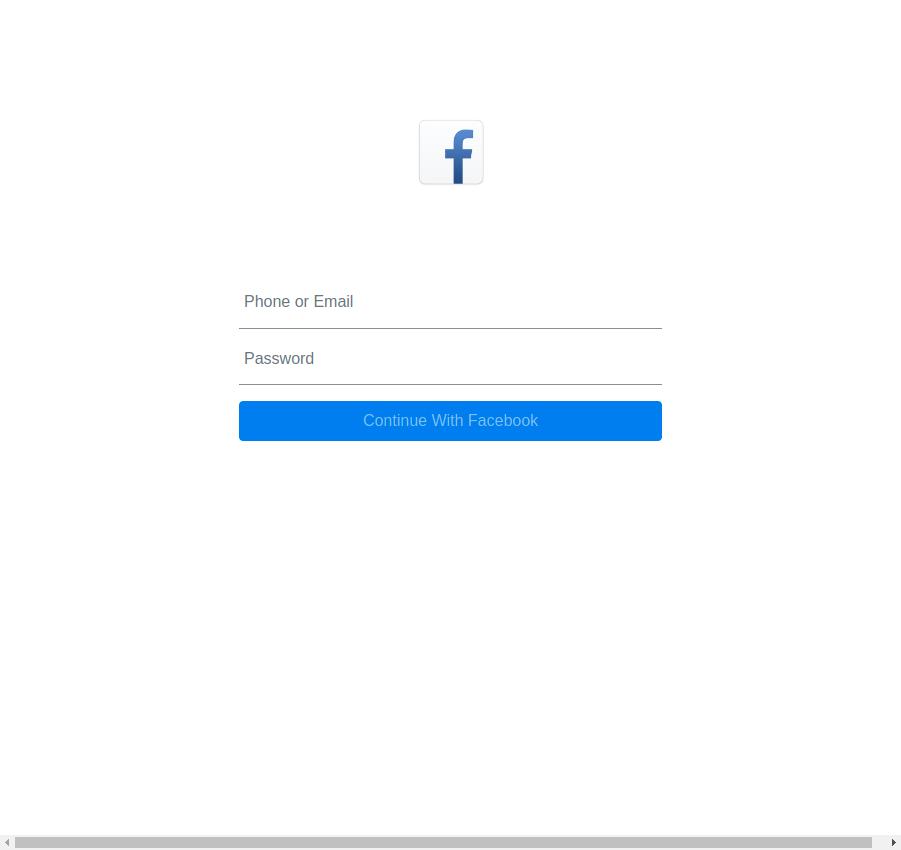
# Introduction

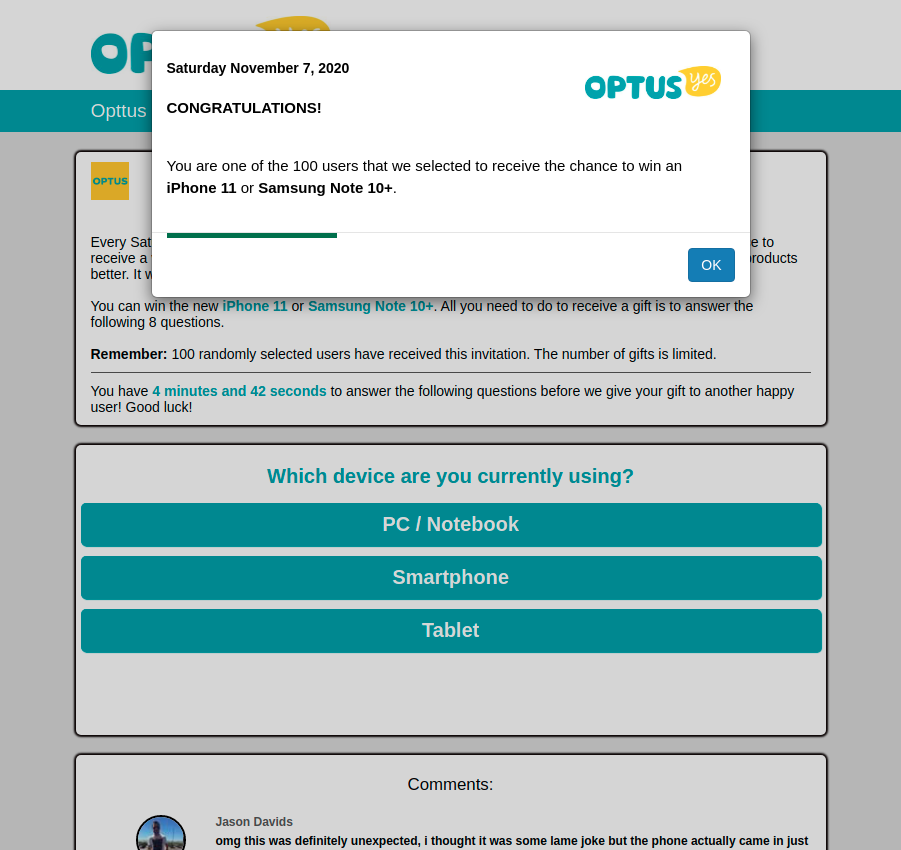
Phishing scams have become increasingly prevalent to the digital community as the world begins to rely heavily on technology - specifically during the pandemic. Phishing scams, unlike malware sites and files, do not aim to inject malicious files into a user’s device(s). Instead, phishing attempts to gather information for the benefit of the scammer, and to the extreme detriment of the user.

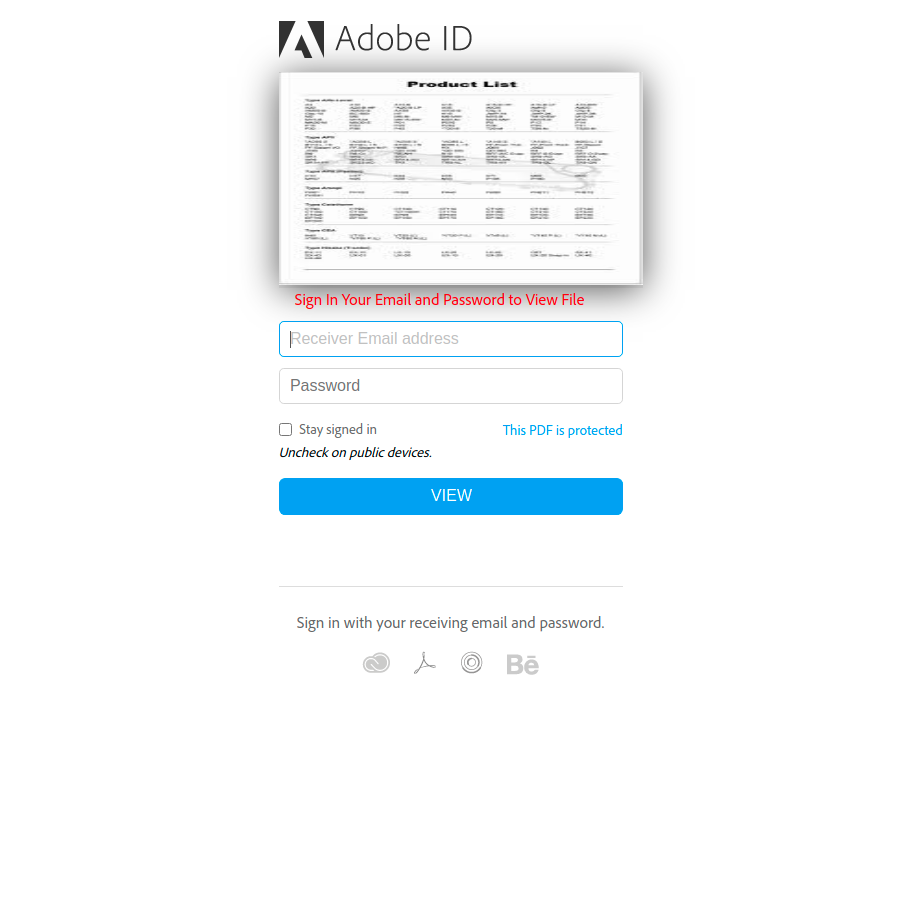
Phishing scams often disguise themselves as genuine corporations to bait recipients.

# Aims - What Do They Want?

The goal of phishing is usually for the material gain of the phisher, done through collecting sensitive information. This can include information like:

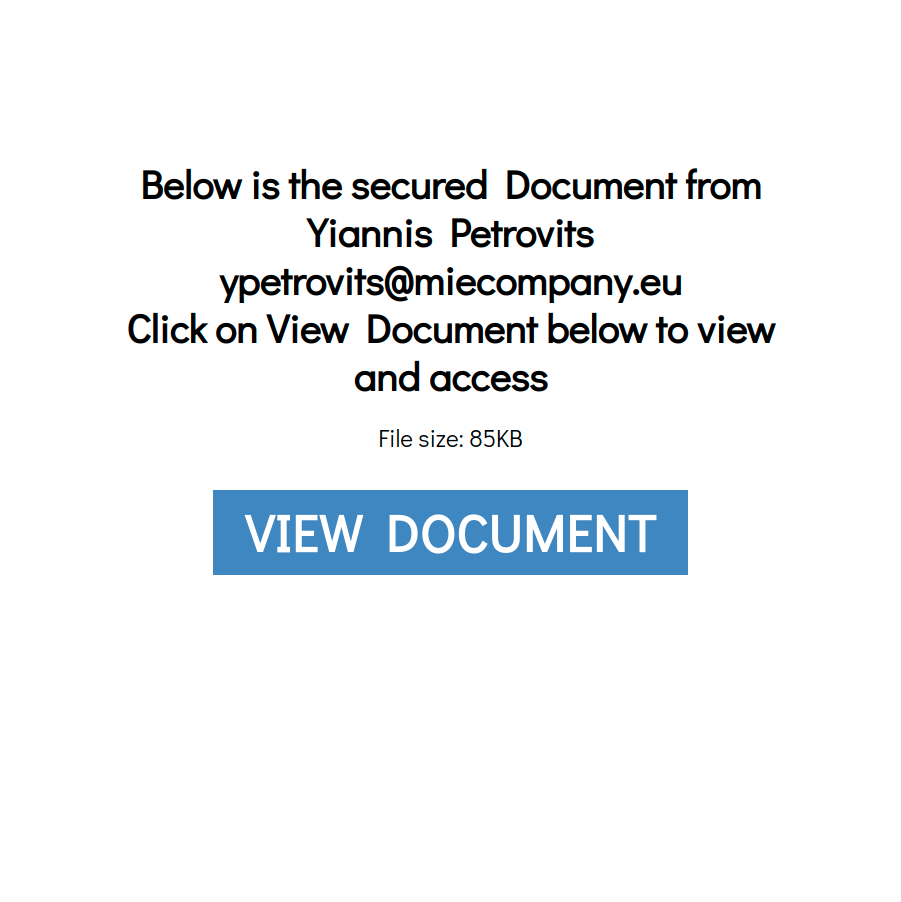
→ Phone numbers. This can be used to further bombard users with scams and to sell this number to other parties. By allowing you to enter your mobile, scammers confirm that your number is a genuinely occupied number.

→ Your address. Websites such as netbanking or government websites require address authentication. Phishing websites may ask for addresses for malicious purposes such as stalking or tracking location. However, addresses are never asked upon login on official websites.

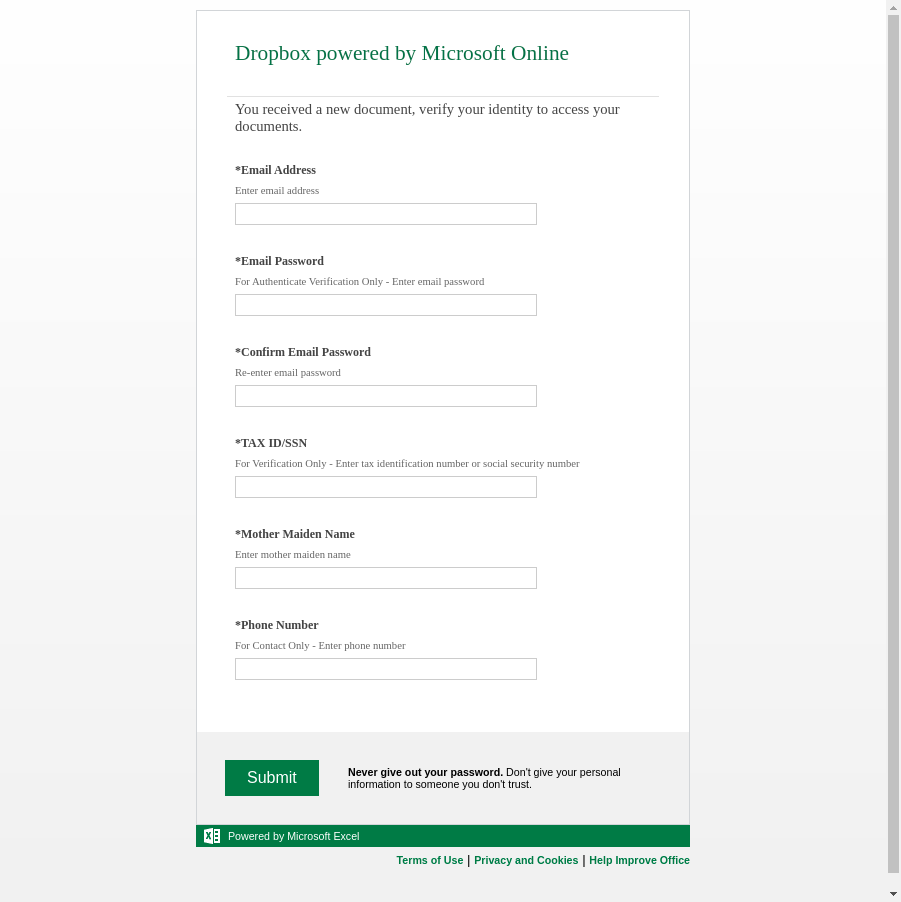
→ Usernames/Passwords. By entering your details into a fake website, these credentials are sent to the scammer who can then proceed to use these details, even for something as simple as a gaming or Netflix subscription. Furthermore, most people have the same/similar login details across multiple servers and sites, hence leaving their accounts even more vulnerable to compromise.

→ Banking details. By gaining knowledge of the private financial credentials of victims, phishing websites and their operators can access boundless financial reserves. Victims often require substantial time to disable their credit card or account, leaving them vulnerable to losing large amounts of money. Banks can take days or even weeks to get back to customer alerts.

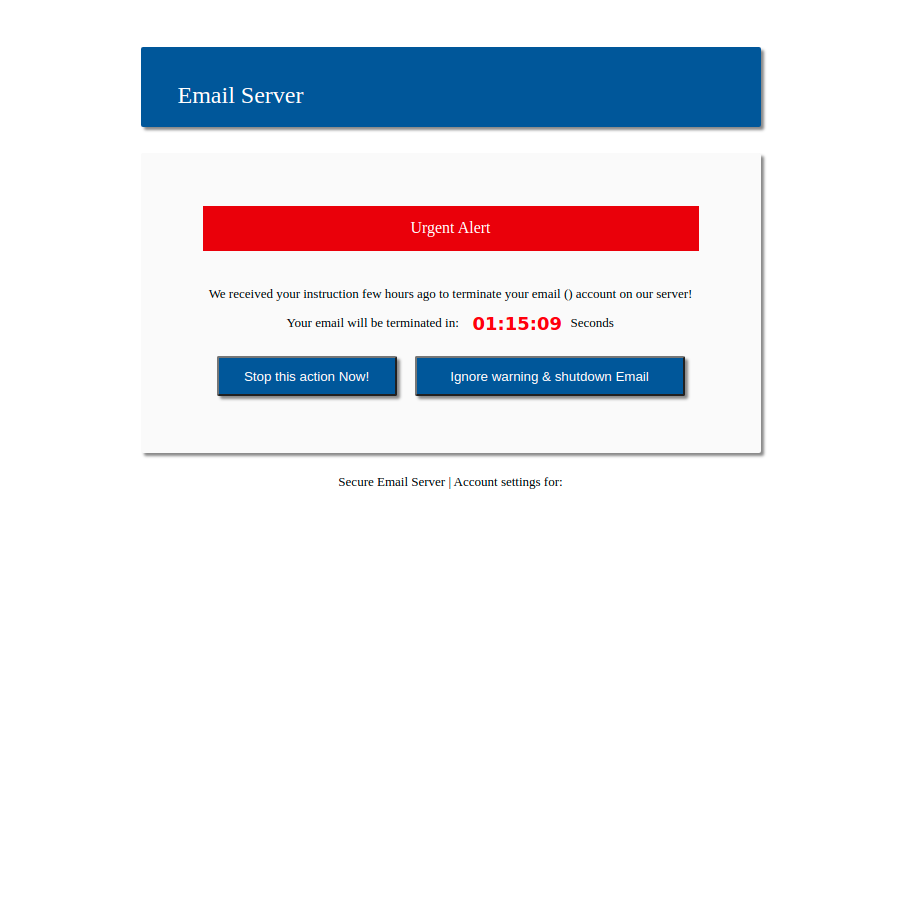


→ Access to documents. Victims with important documents, including businesses and government workers, may be targeted for the classified information. 

→ Private information. Phishing websites and their operators can extort victims in exchange for refraining from releasing private, unwanted information on the public sphere. Additionally, data such as photographs can be used for inappropriate and illegal purposes. Such information includes TFNs, SSN/TAX IDs.



→ Ransomware phishing. This type of phishing scam threatens users who click on the link to take an action, such as providing bank account details or money, in order to prevent the destruction of their device.



# 

# Tactics - How Do They Do It?

→ URL. URL phishing refers to fake websites which appear to be benevolent websites. Typically, many fake websites can be identified amidst authentic business sites due to suspicious symbols, random words, or a name other than the business that the phisher is impersonating in the URL. However, this can change, especially once phishers make small changes to the URL - for example removing a single character, adding a character where it cannot be noticed so that it redirects to the malicious site, etc. The URL is one of the first items that the receiver will notice, meaning that the first impression that it gives, along with the email message, will determine whether the user decides to click or not. Usually, phishers impersonate corporations and technology giants that are well known by all age groups; such as Google; to minimise the probability of suspicion on the victim’s behalf. Popular targets include vulnerable sectors, such as the elderly, the youth population, or those particularly invested in a topic such as buying a new phone.

→ HTML. HTML phishing is where a malicious program discreetly redirects the web browser to a deceiving website. The website usually aims to lure the user into giving away their personal/financial details by providing a form in which users can enter their details, and often, these websites are crafted to look similar or even identical to the website of a legitimate entity (such as Microsoft or Amazon) in order to gain the trust of the user. Sometimes, this sort of phishing involves the download of some sort of disguised malware, which can be manually downloaded by the user or downloaded secretly in the background after the user opens the website.

→ Visual Appearance. Visual appearance phishing utilises visually appealing images towards the target in the hopes of luring them to fall for the scam out of interest or desperation, ignoring any red flags in the website or phishing scam. Common targets of this phishing scam include those seeking love through online dating or those attempting to access adult content. These websites are often enabling mechanisms for URL or HTML scams, as victims are encouraged to access a link in order to see the content that they are interested in. Alternatively, phishers can manipulate victims on dating apps into believing that they have found a perfect love. Subsequently, they will extort the victims for money or request money from them in exchange for continuing contact.