Task 2: Analyze a Phishing Email Sample.

Sample phishing email…

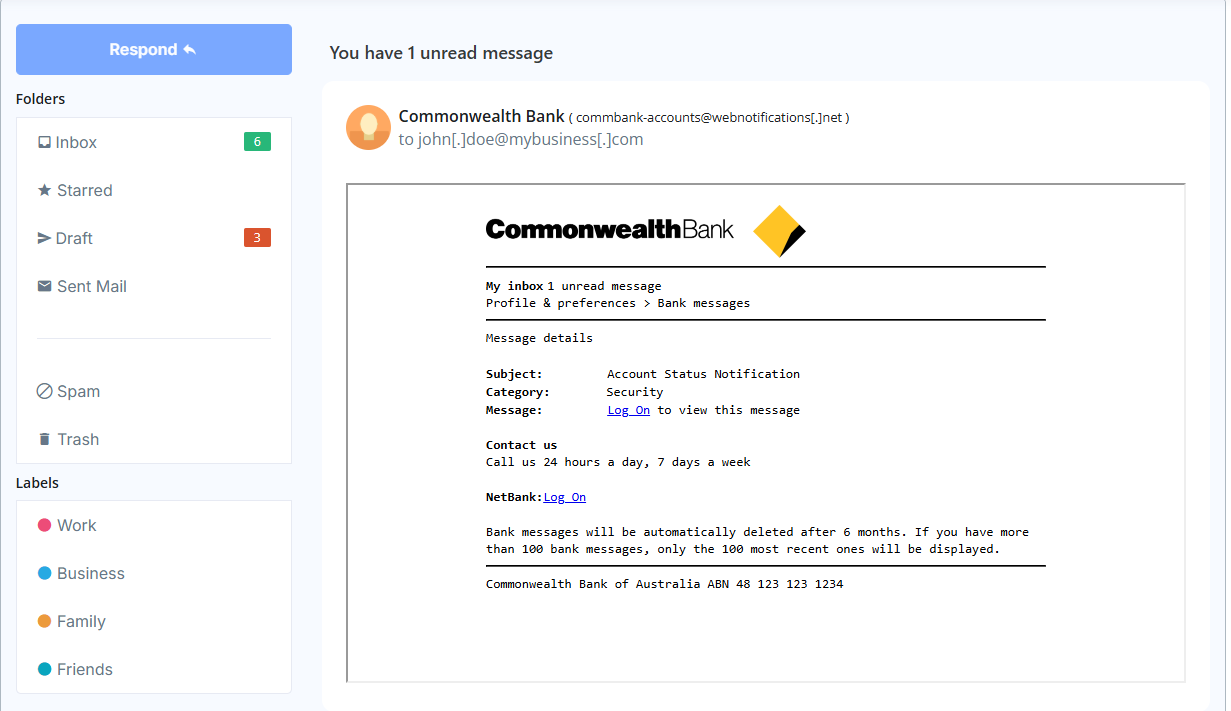


Figure 1 - Phishing example 1 from caniphish.com

Figure 1 is an example of phishing email regarding bank notification, where the attacker has created this email with detail leaving no trace for mistake. But if a victim is not new at getting phishing email, then the person will point out that normally banks would not send login link with the notification.

Upon clicking the log on link following page will show up…

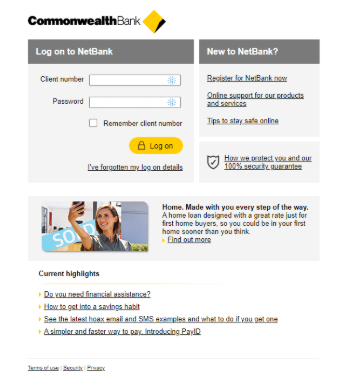


Figure 2 - Phishing page upon clicking log on link

Now if you mistakenly enter log on details then the page will simply do nothing other than loading prompt and the attacker will gain your bank log on credentials. A normal person will fall into this trap, but a malware educated person will not.

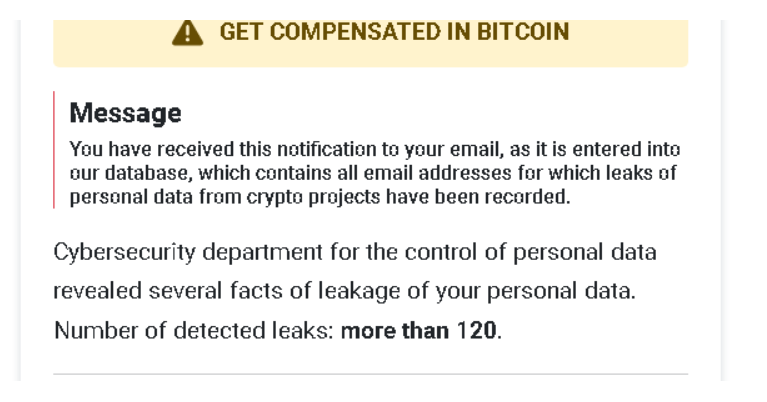
Additionally, an email will have header and footer aligned with the information within the email. A non-phishing email will have message with symmetrical information and attachments.

Now we will examine another phishing email from crypto wallet.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a phone

AI-generated content may be incorrect.

A close-up of a logo

AI-generated content may be incorrect.

As you can see this email have good header but improper footer, and it has urgent or threatening language body. This email looks suspicious upon examining the attachments. This email might lead you to malicious page where it can gain your IP or MAC address and other important details. This would be the reconnaissance stage for attacker and might do social engineering to the victim.

Most victims do not scroll down to the end of email that’s where you can easily identify phishing email.

**Common phishing traits found in email:**

* Misspelled words or poor grammar.
* A suspicious or unfamiliar link.
* An unusual greeting or salutation.
* An unusual email address for the sender.
* A lack of specific details about the alleged activity.
* A generic or impersonal tone.
* An unusual email address for the sender.
* An overly urgent tone with strong language.
* A demand for immediate action with consequences.
* A lack of personal information in the email.
* A lack of security measures, such as encryption.
* An unexpected attachment or document.
* A lack of proper formatting or information in the document.
* A suspicious link.

There are various methods to identify emails or malicious emails. Software like Autopsy, Magnet Axiom, Aid4Mail, FTK, MailXaminer. Furthermore there are online tools for quick examination.

NOTE:

The phishing samples are from

<https://caniphish.com/email-phishing-simulator?email=CommBank-Unread-Message#emailTitle>

<https://github.com/rf-peixoto/phishing_pot.git>

Software used

<https://www.emlreader.com/>