Ongoing threat of COVID-19-related online scams and increased risk of notifiable data breaches

Source: https://www.scamwatch.gov.au/news/covid-19-coronavirus-scams

https://www.who.int/about/communications/cyber-security

Date: 2 April 2020

Abstract:

Cybercriminals are using the global COVID-19 emergency to perpetuate online scams. These scams include selling coronavirus-related products online, and using fake emails or text messages to try and obtain personal data.

If staff within an organisation become victim to an online phishing scam, there is a distinct possibility that there will be a data breach from within the organisation. If a data breach occurs, the organisation may have to consider whether the data breach is a notifiable data breach under the *Privacy Act 1988.* For more information on data breaches and what might be a notifiable data breach, see our Practical Guidance on the data breach notification regime.

Organisations therefore should educate staff about the ongoing threat of COVID-19 related online phishing scams and steps to take if they think they have been targeted by scammers.

Common examples of COVID-19 related scams

- phishing emails and phone calls impersonating entities. These include the World Health Organisation ('WHO'), government authorities, people confirmed to have the coronavirus, and legitimate businesses such as travel agents and telecommunications companies
- people receiving misinformation about the coronavirus, being sent by text, social media and email (including voice message phishing emails)
- products claiming to be a vaccine or cure for the coronavirus
- investment scams claiming coronavirus has created opportunities
- links to 'more information'

Steps to take

1. **Verify the sender by checking their email address**

   Make sure the sender has an email address such as 'person@who.int' If there is anything other than 'who.int' after the '@' symbol, this sender is not from WHO.

   For example, WHO does not send email from addresses ending in '@who.com' , '@who.org' or '@who-safety.org'.

2. **Check the link before you click**

   Hover your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Better still, navigate to the website you want to reach directly, by typing the website address into your browser.

3. **Watch for spelling and grammatical mistakes**

If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.

4. **Look for generic greetings**

   Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.

5. **Be careful when providing personal information**

   Always consider why someone wants your information and if it is appropriate. There is no reason someone would need your username & password to access public information.

6. **Do not rush or feel under pressure**

   Cybercriminals use emergencies such as COVID-19 to get people to make decisions quickly. Always take time to think about a request for your personal information, and whether the request is appropriate.

7. **If you gave sensitive information, don't panic**

   If you believe you have given data such as your username or passwords to cybercriminals, immediately change your credentials on each site where you have used them.

8. **If you see a scam, report it.**

   If you think you have been scammed, refer to your internal online scam reporting processes. You can also make a report on the Scamwatch website, and find more information about where to get help.