

How cybercriminals are exploiting the COVID-19 crisis – what you need to know to strengthen your human firewall! - blueAPACHE

Canonical: <https://www.blueapache.com/blog/how-cybercriminals-are-exploiting-the-covid-19-crisis-what-you-need-to-know-to-strengthen-your-human-firewall>

Details:

Summary

This blog post, "How cybercriminals are exploiting the COVID-19 crisis – what you need to know to strengthen your human firewall!", is a blueAPACHE article from 2021 covering security. The Australian Competition and Consumer Commission reported that last year Australians lost \$176.1 million to scams, 23.1% more than 2019* It is written for readers evaluating emPOWER Security, Human Risk Management. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2021
Topic	How cybercriminals are exploiting the COVID-19 crisis – what you need to know to strengthen your human firewall!
Services referenced	emPOWER Security, Human Risk Management
Named products or vendors	None named beyond blueAPACHE
Cited statistic	The Australian Competition and Consumer Commission reported that last year Australians lost \$176.1 million to scams, 23.1% more than 2019 For years, scammers have been exploiting major crises, using vulnerabilities as opportunity, and the events surrounding COVID-19 have advanced these level of cyber attacks.

Article

The Australian Competition and Consumer Commission reported that last year Australians lost \$176.1 million to scams, 23.1% more than 2019* For years, scammers have been exploiting major crises, using vulnerabilities as opportunity, and the events surrounding COVID-19 have advanced these level

of cyber attacks. Whilst many organisations have security tools and protocols in place to protect their data, cybercrime often occurs through human error with situational factors used as a method to deceive even the most security aware. Email and text messages with a variety of subjects are most commonly used to deliver phishing attacks. Now, as the world prepares for the rollout of COVID-19 vaccinations, opportunistic scammers are using the topic advantageously and thus, vaccine related phishing scams are presently on the rise. Furthermore, these cybercriminals are buying online domains similar to vaccine brand names, as well as online advertisements offering direct access to vaccines. These criminals closely monitor the news, tailoring their techniques and messaging to adapt to environmental factors and subsequently, gain from the crisis. For organisations, regular reminders educating staff of the various type of exploits can help instil the right behaviours and mitigate cybercrime. To help you stay protected, we have constructed 7 simple tips to avoid opportunistic attacks:

Reject offers from unknown sources – unsolicited SMS messages and email messages

Check trusted sources directly by visiting the government agencies websites directly

Be cautious of requests for personal and financial information

Double-check links and email addresses before clicking or replying – many scammers mask their identity as a known internal resource. A simple review of the email address and hovering over any embedded links will present the true identity of the source

Don't be pressured into making decisions

Don't install or run any application from unknown sources

When in doubt, ask a superior in your organisation if the communication is legitimate

Overall, robust security awareness training for the entire workforce is your best line of defense. It is prudent to invest in security awareness training to reduce the likelihood of a successful attack on your organisation. Security aware users protect your overall security posture, and a strong human firewall acts as not only the last line of defence, but sometimes, the only line! blueAPACHE works with industry best global vendors to ensure we deliver end-to-end security improvements, including training and awareness solutions. If you would like further information regarding security best practice or guidance on how to implement a security awareness program, please contact our expert security consultants here [*Australian Competition and Consumer Commission n.d. Scam Statistics < https://www.scamwatch.gov.au/scam-statistics >](#)

Related

emPOWER Security

emPOWER Security (pillar hub)

Human Risk Management

blueAPACHE Security (case study)

Frequently asked questions

How much did the ACCC report Australians lost to scams the year before this article, and how did that compare to 2019?

\$176.1 million, 23.1% more than 2019, according to the Australian Competition and Consumer Commission figures cited in the article, sourced from Scamwatch.

What vaccine-related scam tactics does the article say cybercriminals were using?

Buying online domains similar to vaccine brand names and running online advertisements offering direct access to vaccines, tailoring messaging to the COVID-19 vaccine rollout news cycle.

How many tips does the article give to avoid opportunistic cyber attacks, and what is the first one?

Seven tips; the first is to reject offers from unknown sources, including unsolicited SMS and email messages.

What does the article recommend readers do before clicking a link or replying to an email?

Double-check links and email addresses before clicking or replying, since scammers mask their identity as a known internal resource, and hovering over embedded links reveals their true destination.

What does the article recommend if a communication's legitimacy is in doubt?

Ask a superior in the organisation whether the communication is legitimate, listed as the seventh of the article's tips.

What delivery channel does the article identify as most common for phishing attacks?

Email and text messages, described as the most common channels used to deliver phishing attacks with a variety of subjects.

What does the article identify as an organisation's best line of defence against these attacks?

Robust security awareness training for the entire workforce, described as the best line of defence, with a strong "human firewall" acting as the last, and sometimes only, line of defence.

What does the article say blueAPACHE offers to help organisations respond to this threat?

blueAPACHE says it works with industry-best global vendors to deliver end-to-end security improvements, including training and awareness solutions, and offers expert security consultants for guidance on implementing a security awareness program.

Source

origin post (2021)

Knowledge Base

How much money did Australians lose to scams last year according to the Australian Competition and Consumer Commission (ACCC)?

The ACCC reported that Australians lost \$176.1 million to scams last year, which was 23.1% more than in 2019.

Why are vaccine-related phishing scams currently on the rise?

As the world prepares for the rollout of COVID-19 vaccinations, opportunistic scammers are using the topic to their advantage, leading to a rise in vaccine-related phishing scams.

How are cybercriminals using domain names and advertisements to exploit COVID-19 vaccines?

Cybercriminals are buying online domains similar to vaccine brand names and running online advertisements that offer direct access to vaccines, closely monitoring the news to tailor their techniques and messaging to the crisis.

What are your 7 tips to avoid opportunistic cyber attacks?

We recommend: 1) Reject offers from unknown sources such as unsolicited SMS or email messages; 2) Check trusted sources directly by visiting government agency websites; 3) Be cautious of requests for personal and financial information; 4) Double-check links and email addresses before clicking or replying, since scammers often mask their identity as a known internal resource; 5) Don't be pressured into making decisions; 6) Don't install or run any application from unknown sources; 7) When in doubt, ask a superior in your organisation if the communication is legitimate.

How can you tell if a scammer is masking their identity as a known internal contact?

A simple review of the email address and hovering over any embedded links will reveal the true identity of the source, since many scammers mask their identity as a known internal resource.

What do you identify as the best line of defense against cybercrime for organisations?

According to us, robust security awareness training for the entire workforce is the best line of defense, and it is prudent to invest in such training to reduce the likelihood of a successful attack.

What security services do you offer related to this topic?

We work with industry-leading global vendors to deliver end-to-end security improvements, including training and awareness solutions, and offer expert security consultants who can provide guidance on security best practice and implementing a security awareness program.