Cybercrime in the time of Coronavirus: Everything You Need to Know

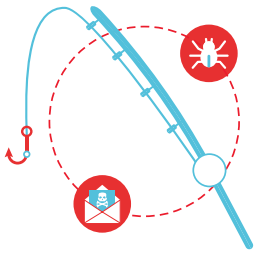
INSTITUTE OF advanced cyber defence

in partnership with Cybint Cyber Solutions

The impact of the coronavirus is unprecedented. We are experiencing a global crisis of historic proportions. We are having to change the way we work, learn, travel, and interact with one another. The changes are also leading to increased online security risks for both individuals and organisations, as millions have been forced to work and study from home, interacting more online than in person. The consequence? Cybercrime and cyber-attacks are on the rise.

Using current events and social trends to spread malware and maximise the impact of dissemination of malicious campaigns is nothing new in the world of cybercrime. For the past few weeks, cybercriminals have exploited the coronavirus for Social Engineering campaigns designed to infect online accounts and systems - and as the virus spreads in the real world, so too will its impact online.

In this challenging time, it's important to know how to protect yourself and your organisation from the increasing risk of cyber-attacks. This article offers a short review of some of the major coronavirus-themed cyberattacks used around the world, along with some strategies for better online safety:



Phishing Scams

Phishing scams are attacks in which a hacker/criminal impersonates a legitimate certified entity to steal sensitive information, install malicious malware on the user's computer, or cause damage.

Recently many cybersecurity and cyber intelligence companies have reported a significant increase in the number of phishing attempts purporting to provide updates about the coronavirus. For example, the cybersecurity firm Check Point reports that coronavirus-themed domains are 50% more likely to be malicious than other domains. Cyber-criminals are no doubt aware that people are hungry for up-to-the-minute information about the virus and its spread, and maybe eager to click on any link that promises them such information. As Check Point notes, "Hackers around the globe have found the coronavirus serving them well as an enabler of their activities, and are still riding the wave of the epidemic."

Successful phishing messages may be hard to distinguish from real messages which is why we listed below some of the most common signs of phishing.

Common Signs of a Phishing Attempt:

- Misspelled URLs – If you get a message purporting to be a legitimate organisation, confirm that any link in the message matches that organisation's official URL before clicking on it. For example, the World Health Organization (WHO) reported suspicious email messages about the COVID-19 emergency pretending to come from them.
- Requests for sensitive information – These can include requests for passwords, financial information. usernames, or credit card numbers. Avoid providing unnecessary personal information, and consider why the sender is requesting it and if sharing it is appropriate.
- Spelling and grammatical errors: Another potential giveaway is the use of unusual wording and generic, non-personalised greetings, such as "dear customer."
- Unusual senders: Another red flag is if the message comes from an unexpected sender, such as someone the receiver does not know or does not communicate with regularly.
- Suspicious links – Check any links before clicking on them by hovering your cursor over the link–this may show it points to a fraudulent site.

Summary

The Coronavirus crisis is not only a health issue.
It is changing the way we work, learn, travel, and interact with one another.

Keeping safe in this new situation requires us to be vigilant to digital threats, cyber-attacks and online crimes as well. This is true for our organisations, ourselves and our loved ones, including our children who learn from home and spend a significant amount of time online. The Coronavirus (COVID-19) is causing a global crisis of historic proportions - it's not only changing the way we work and interact with each other, but also increasing online security risks for both individuals and organisations. It's no surprise with millions becoming quarantined and working from home on their own devices that cyber-attacks are on the rise.
Please join us for this brief educational webinar session on protecting your business from cybercrime. We encourage managers to invite their colleagues and team members to learn best practices and strategies for avoiding cyber-attacks during remote work and quarantine.

The **Institute of Advanced Cyber Defence** aims to advance both the quantity and quality of knowledge and skills in the domain of cyber intelligence and security. The Institute's expertise is based on first-hand experience protecting organisations from cyber threats and attacks, as well as on the expertise of a network of companies from tier-1 countries that are global leaders in advanced cyber defence services and solutions. Their offerings are military-grade and find their origins in law enforcement and national security, with their team members often having served in leadership positions in the world's elite national cyber defence units. As such, our pedigree is unmatched and with our partners we seek to further develop and transfer this know-how for the benefit of individuals and organisations alike via a number of avenues.

Cybint is The Institute of Advanced Cyber Defence's global education partner. Cybint is an international cyber education leader committed to solving the significant global shortage of cyber security experts and putting an end to the growing threat of cyber crimes, by helping financial institutions, companies, government agencies and universities to develop cyber security and intelligence capabilities.

In certain circumstances we call on experts from other partners like providers of amongst others cyber intelligence and security consulting services, data mining solutions, as well as breach attack simulation software.