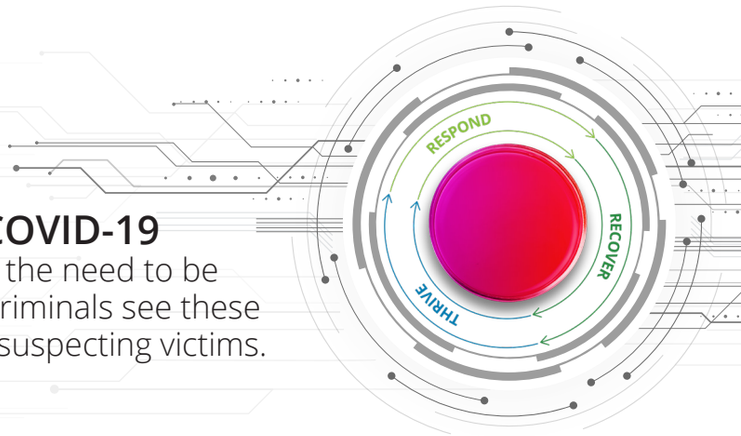
Deloitte.



Cyber Awareness in the time of COVID-19

In a world where panic is rife and users feel the need to be informed about the COVID-19 virus, cyber criminals see these conditions as an ideal platform to attack unsuspecting victims.

Cyber criminals...

...will aim to **steal information or cause massive damage** such as triggering ransomware attacks that encrypt all information for which they demand a ransom before allowing the organisation to unencrypt their data.

...use **online social interaction as a means to persuade individuals to comply** with a specific request to compromise information, and specifically login credentials, so that they can use these to illegally access systems and information.

...are **impersonating official websites** such as the World Health Organisation (WHO) or the National Institute for Communicable Diseases (NICD), creating domains similar to the NICD's website to steal email credentials and even request Bitcoin donations to allegedly fund a vaccine.

...will use the **human sense of compassion to trick victims into acting on their requests**, and will do this using messages about their loved ones and family. They will utilise phishing schemes to elicit a sense of fear and urgency to get victims to comply with their requests.

Here are some tips to keep safe and create awareness:

Make users aware that they should look out for spam e-mail messages that may look legitimate or purport to be from official sources and may use subject line themes associated with COVID-19 as these may trick victims into divulging information or visiting malicious websites.

Create awareness to avoid clicking on attachments or links embedded in email messages with subject lines purporting to contain information related to COVID-19 or Coronavirus or any other messages to entice them, as these sites may attack their machines and information, or attempt to trick them to divulge usernames and passwords.

Recipients of suspicious emails should be encouraged to verify the sender via alternate communication methods and not use the contact information provided in a message.

Make users aware that they should not let fear and emotion trick them into not using common sense when evaluating communication regarding COVID-19.

Use firewalls and intrusion detection/ prevention systems (IDS/IPS) to detect and block network communications with malware Command and Control (C2) nodes.

Consider alerting based on emails containing references to COVID, Coronavirus, and other keywords which contain uncommon file types such as iso, arj.

Consider alerting based on COVID-19 related domains on commonly abused hosts (Cloudflare, GoDaddy, OVH), name servers (NameCheap) and unusual top level domains (e.g. .tk, .pw etc.)

Deploy intrusion detection security controls such as Snort or Suricata on the network to detect malicious activity during post-exploitation.

Enable and configure Windows Audit Policy and Logging and set the registry to enable process command-line logging.

Ensure regular, offline backups are done and the backups are regularly tested for all critical systems and data to mitigate potential ransomware attacks.

Do not issue payments for ransomware as the adversary is under no obligation to restore files which may not be recoverable even after acquiring the required encryption key.

Disallow auto-saving to user "Downloads" folder and disable the ability to execute an application or opening a data file from that location.

Use Active Directory Group Policy to block users from enabling macros in any Microsoft Office applications.

Enable sufficient logging of host and user activity that can be leveraged and analysed for suspicious threat actor activity or attempts to compromise hosts and/or user accounts.

Ensure remote working is conducted through a secure VPN enabled with strong authentication measures such as multi-factor authentication.

For more information and assistance on any incidents and issues experienced, please contact:
Eric Mc Gee erimcgee@deloitte.co.za | Cathy Gibson cgibson@deloitte.co.za | Tiaan van Schalkwyk tvanschalkwyk@deloitte.co.za