National Cyber Security Centre

Working Remotely: Advice for Organisations and Staff

New Zealand's National Cyber Security Centre is hosted within the Government Communications Security Bureau

March 2020

Thinking Ahead, Being Prepared

The National Cyber Security Centre (NCSC) is co-ordinating closely with our partner agencies to prepare for the possible cybersecurity impacts of a COVID-19 outbreak in New Zealand. This document has been compiled to help organisations think about the cybersecurity risks that arise when staff need to work from remote locations. We've provided a series of recommendations that can be used as a starting point in addressing these risks.

The NCSC is aware of malicious cyber activity seeking to exploit public concern surrounding COVID-19. It's important to note that remote access solutions may be specific targets of cyber criminals and other hostile actors.

Cybersecurity Advice for Organisations

Organisations planning a capability for staff to work remotely, or planning to increase the number of their staff who currently do so, should consider the cybersecurity implications of these arrangements. The NCSC recommends taking the following steps:

- Maintain an awareness of the risks and mitigations associated with flexible worksite arrangements.
- Be aware that bring your own device (BYOD) solutions utilised by employees may not have the same protections as corporate devices.
- Liaise with your IT department to provide staff working remotely with advice on the correct security settings for their devices.
- Focus on securing systems that enable remote access, such as VPNs. Ensure these systems are fully patched, firewalls are properly configured, and anti-malware and intrusion prevention software is installed.
- Test the capacity of your remote access solutions in advance. Develop strategies to increase this capacity if necessary.
- Wherever possible, multi-factor authentication for remote login or cloud-based corporate applications must be implemented.
- Ensure staff working remotely have good awareness of—and access to—the information technology support mechanisms in place for them.

- The use of unauthorised software for official purposes (known as shadow IT) can increase when working remotely, increasing security and privacy risks. Ensure staff are aware of the policy, privacy and legal obligations that apply to your organisation's information.
- Only ask staff to perform remote functions that are supported by your organisation's IT capabilities.
- Examine your incident response plans and, if necessary, update these to account for staff working remotely.
- Review your business continuity and contingency plans. Ensure these are up to date.
- Assess your organisation's supply chain for possible disruption resulting from COVID-19. Identify possible substitute products or alternate supply sources.
- Use trusted sources such as New Zealand Government websites for up-to-date information about COVID-19. Monitor the NCSC's website for information on cyber threats and vulnerabilities.
- Government agencies should review the Protective Security Requirements and the New Zealand Information Security Manual for existing information on working remotely.

Cybersecurity Advice for Remote Workers

- Avoid clicking on any links in unsolicited emails and be very cautious of email attachments. Malicious cyber actors may seek to use the concern around COVID-19 as an opportunity to conduct phishing attacks, in which they use emails and fake websites to trick victims into revealing sensitive information.
- Do not provide personal or financial information in emails, texts, or instant messages, and do not respond to requests for this information.
- When working remotely, ensure you do not leave your devices unlocked in public places, such as coffee shops or public transport. Consider avoiding working in public places altogether.
- The use of unsecured public Wi-Fi poses a significant security risk. Sensitive data you transmit through these networks may be intercepted and exploited by malicious actors.
- Review CERT NZ's advice and guidance on COVID-19 themed scams and staying secure while working from home.