National Computer Board

CERT-MU

# CERT-MU Security Alert

## Embracing and Securing a Remote Workforce: Cybersecurity in The Time of Covid-19

**Original Issue Date:** 24 March 2020

**Description:**

As the crisis around the coronavirus (COVID-19) continues to expand around the world, including in Mauritius, organisations are facing sudden and profound challenges as they seek ways to quickly support directives from employees to vacate offices and start working from home. As enterprises and organisations rush to shift their businesses, cybercriminals are ramping up their tactics to take advantage of those who may have inadequate or naïve security postures. Given the challenges in securing work from home-environments, the attack surface represents an attractive opportunity for threat vectors. Maintaining security in the face of this global office exodus presents significant risks for most organizations.

In this crisis situation where Mauritius is fighting against the COVID-19, CERT-MU will be posting contents regularly that will help you to embrace and secure a remote workforce. Aside from the pressure this office exodus puts on IT teams, network architectures and even equipment suppliers, there are real cybersecurity challenges organisations need to consider.

## Seven key factors that can help ensure remote worker cybersecurity:

1. **Keep close contact with your employer**

It is smart to stay on top of company communications. Your inbox might contain emails about policy changes ranging from work hours to travel. Your employer might consolidate coronavirus-related information on the company intranet. Companies around the world continue to react to developments around the COVID-19 pandemic. It is important to know new policies to help keep you, your coworkers, and the business safe.

2. **Use your company's tech toolbox**

Companies often have tech tools that can help keep you cybersafe when you work from home. That might mean you do your work on company-supplied laptops and mobile devices. They likely include firewall and antivirus protection, along with security features like VPN and 2-factor authentication. Your employer's cybersecurity tools are designed to protect data and devices. Cybercriminals have an interest in both, whether you are working in the office or at home.

3. **Control the impulse to improvise**

Employees often work in teams, and that can mean using collaboration tools like instant-messaging platforms and video-meeting rooms. If a tool is not working right, you might be tempted to download a substitute. It is advised to refrain to do so. You could inadvertently introduce a software program with a security flaw — and that means someone unauthorised may be able to access company data, or any personal data you have on that device.

4. **Stay current on software updates and patches**

You might get reminders that software updates are available for your computer, laptop, tablet, or mobile device. Do not wait and update to have the latest software on your computer or laptop. Also, keep in mind you can configure your devices to update automatically. Updates help patch security flaws and help protect your data. Updates can also add new features to your devices and remove outdated ones.

5. **Keep your VPN turned on**

A VPN (Virtual Private Network) can help protect the data you send and receive while you work from home. A VPN can provide a secure link between employees and businesses by encrypting data and scanning devices for malicious software such as viruses and ransomware. VPNs help to protect against cybercriminals from seeing what you do online during a workday. That might include sending or receiving financial information, strategy documents, and customer data. A VPN helps keep that information secure from cybercriminals and competitors.

6. **Beware of coronavirus-themed phishing emails**

Cybercriminals are exploiting the coronavirus outbreak to send fake emails with dangerous links to employees. The email messages may appear to come from company

officials and might ask you to open a link to a new company policy related to the coronavirus. If you click on the attachment or imbedded link, you are likely to download malware onto your device. Do not click. Instead, immediately report the phishing attempt to your employer.

7. **Develop a new routine**

Working from home requires changing your routine. Making sure you are cyber secure is part of that. But it also involves structuring your day to work efficiently and maintain contact with your team. If you are used to starting the day by greeting your coworkers, you might consider continuing to do that by email or on a chat platform. It is easy to lose focus or feel isolated when working from home. Take steps to avoid letting that happen. Reach out and stay engaged with your colleagues. The coronavirus may have changed your work life, but you still have a job to do.

## BE CYBERSAFE FROM THE CORONAVIRUS INFECTIONS

For more information, please contact the CERT-MU Team.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

**Hotline No:** (+230) 800 2378
**Fax No:** (+230) 208 0119
**Gen. Info**. : contact@cert.ncb.mu
**Incident:** incident@cert.ncb.mu
**Website:** http://cert-mu.org.mu