

# Coronavirus and Cyber Security



**By now it is clear that COVID-19 has a significant impact on countries, organisations and citizens around the world. Each country is implementing its own response, with The Netherlands choosing to minimise social contact (*social distancing*), work from home as much as possible and close most public establishments. This could very well impact the cyber security position of organisations.**



**Ruud Verbij** MSc PCIP  
is Cyber Governance and Risk  
Manager at KPMG Netherlands.  
verbij.ruud@kpmg.nl



**Koos Wolters** RE CISA  
is Lead Partner Cyber Security at  
KPMG Netherlands.  
wolters.koos@kpmg.nl

For many people, social distancing is not an easy task, having to juggle home and work responsibilities, exacerbated for many by the fact that schools and daycare centres are also closed. On top of that, organisations need to be aware of the heightened cyber security risks related to remote working in response to COVID-19. We currently see six threats we want organisations to be aware of related to remote working in these times.

## CYBER SECURITY CONSIDERATIONS

**CEO fraud exploiting social distancing.** CEO fraud involves e-mails or phone calls trying to persuade the receiver to transfer corporate funds to other

bank accounts. The requestor claims to be the CEO or other senior company figure being under intense time pressure to get an important payment through. Usually such CEO frauds are detected because the receivers check with their colleagues whether these communications can be trusted. Now that everyone is working from home, we expect these checks to be less solid. Please advise staff with access to corporate bank accounts to keep adhering to the four-eyes principle of money transfers and motivate them to follow the incident management process and escalate irregular communications.

**Insecure remote connections to the office.** Not all organisations are technically prepared to offer (mass) remote working options. IT staff under time pressure might not acquire and offer the most secure solutions. We highly encourage the use of at least two-factor authentication for access to company data, along with secure and solid cloud solutions for collaboration where possible. For collaboration, several companies are temporarily offering their solutions for free (including Microsoft Teams, LogMeIn Emergency Remote Work Kit, Cisco Webex and more).

**Increased personal use of company devices.** When working from home, employees may be tempted to use their company equipment (e.g. laptops or phones) for personal purposes. This may increase the risk of these devices being infected with a virus or malware when visiting less secure (personal interest-related) websites. Lately, adverts on such websites in particular have been known to spread malware. We recommend updating company devices automatically, following the advice of the software vendor. We especially recommend updating browsers and related third-party software (e.g. PDF readers, Flash players and JAVA).

**Employees under financial stress or job uncertainty may pose a risk as insider threat.** With the current economic uncertainty of the COVID-19 measures, employees under financial stress or in danger of losing their jobs might fall victim to the insider threat. Foreign agents or competitors from high-risk countries have been known to exploit such circumstances (e.g. economic uncertainty) when approaching potential victims to e.g. steal key corporate data. We advise to be transparent in your communication, monitor staff well-being closely (remotely), pick-up on ‘cries for help’, and to keep on spotting concerning behavior and meeting that with a solid organizational response (attention, understanding and action). Very good material on the insider threat is the “Critical path to Insider Risk”.

**Confidentiality at home.** While working from home, not everyone in the surrounding is vetted to hear or see confidential information. Children, spouse or room mates may not be aware of the confidentiality level of information they hear or see. We advise to have your staff work in separate rooms as much as possible, and to request staff to have calls using headsets instead of a speakerphone.

#### **Phishing attempts specifically related to COVID-19.**

Since mid-February, we have seen, just like colleagues in our global Cyber network, the rapid build-out of infrastructure by cybercriminals used to launch COVID-19 themed spear-phishing attacks and to lure targets to fake websites seeking to collect Office 365 credentials. Examples of campaigns mounted include:

- COVID-19 themed phishing emails attaching malicious Microsoft documents which exploit a known Microsoft vulnerability to run malicious code
- COVID-19 themed phishing emails attaching macro-enabled Microsoft Word documents containing health information which trigger the download of Emotet or Trickbot malware
- Multiple phishing emails luring target users to fake copies of the Centre for Disease Control (CDC) website which solicit user credentials and passwords (or comparable website in other countries)
- A selection of phony customer advisories purporting to provide customers with updates on service disruption due to COVID-19 and leading to malware download
- Phishing emails purporting to come from various government Ministries of Health or the World Health Organization directing precautionary measures, again embedding malware
- COVID-19 tax rebate phishing lures encouraging recipients to browse to a fake website that collects financial and tax information from unsuspecting users.

There are some key steps you should take to reduce the risk to your organization and your employees, particularly as you move to remote working:

- Raise awareness amongst your team warning them of the heightened risk of COVID-19 themed phishing attacks.
- Share definitive sources of advice on how to stay safe and provide regular communications on the approach your organization is taking to the COVID-19 pandemic.
- Make sure you set up strong passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access.
- Provide remote workers with straightforward guidance on how to use remote working solutions including how to make sure they remain secure and tips on the identification of phishing.
- Ensure that all provided laptops have up-to-date anti-virus and firewall software.
- Run a helpline or online chat line which they can easily access for advice, or report any security concerns including potential phishing.
- Encrypt data at rest on laptops used for remote working given the risk of theft.
- Disable USB drives to avoid the risk of malware, offering employees an alternate way of transferring data such as a collaboration tool.

#### **About the authors**

**Ruud Verbij MSc PCIP** is Cyber Governance and Risk Manager at KPMG Netherlands. He has extensive experience with cyber security strategies, governance, risk management and assurance.

**Koos Wolters RE CISA** is Lead Partner Cyber Security at KPMG Netherlands. His areas of expertise are information security (strategy, governance, policies and awareness) and IT governance, control and optimization.