

Coronavirus client advisory



Cybercriminals exploiting Coronavirus

Public concern and working-from-home mandates are providing opportunities for cybercriminals.

Europe has now closed its borders and it is expected that Coronavirus will continue to trigger widespread disruption globally. In an effort to protect public health, more and more governments have implemented school closures and working-from-home mandates.

CFC's in-house cyber incident response team notes, however, that the public concern about the virus's spread as well as remote working is creating opportunities for cybercriminals. This advisory provides some background on these risks along with some easy-to-implement steps that businesses can follow to avoid falling victim.

Coronavirus increasingly being used in phishing attempts

As new cases of the Coronavirus continue to be reported daily, cybercriminals have been leveraging the situation to take advantage of those looking for information on the outbreak. Scams include the following and are changing each day:

- The Sophos Security Team has spotted emails impersonating the World Health Organization (WHO). The emails ask victims to "click on the button below to download Safety Measure". Users are then asked to verify

their email by entering their credentials, redirecting those who fall for the scam to the legitimate WHO page, and delivering their credentials straight to the phisher.

- Interpol has warned of a large increase in fraudulent websites claiming to sell masks, medical supplies and other high demand items that simply take money from victims and never deliver the promised goods. It is advisable that internet users purchase items only from established and reputable sources.
- There have been reports of airlines and travel companies being impersonated by fraudsters in a bid to either obtain sensitive information, like passport numbers, or install malware on victims' computers. They may say they want to advise you of COVID-19 infected passengers on past flights you've taken or offer discounts on future flights. When in doubt, we advise users to be vigilant when clicking on any links, delete any suspicious emails, and not disclose sensitive information if you are approached unexpectedly.
- Fraudsters are also developing fake charitable donation campaigns which claim to help individuals and communities impacted by the Coronavirus. Any money donated is sent to fraudulent accounts. Again, if you are wanting to support relief efforts, make sure to research the organizations you are looking to donate to.

- A Twitter user has identified another malware campaign purporting to be a "Coronavirus Update: China Operations". The emails have attachments linking to malicious software.

As global concern about the coronavirus grows, it is likely that threat actors will continue to abuse this outbreak to their advantage.

Increased remote working can open gateway to hackers

Remote desktop protocol (RDP), when set up correctly, is a great tool for remote working. However, using it without multi-factor authentication (MFA) enabled or on an insecure network can open the gateway to hackers. In fact, in 2019, 80% of the ransomware attacks we handled were initiated through RDP.



In 2019, 80% of the ransomware attacks handled by CFC's cyber claims team were initiated through RDP.

Businesses that start using RDP for remote working during the outbreak should be aware of some of the cybersecurity risks it can pose and ensure it is being used securely. Employees should always log on within a trusted network and ideally work with their IT department to secure personal devices – and implement MFA – prior to remote working.

CFC recommendations

We suggest implementing the following steps to bolster security:

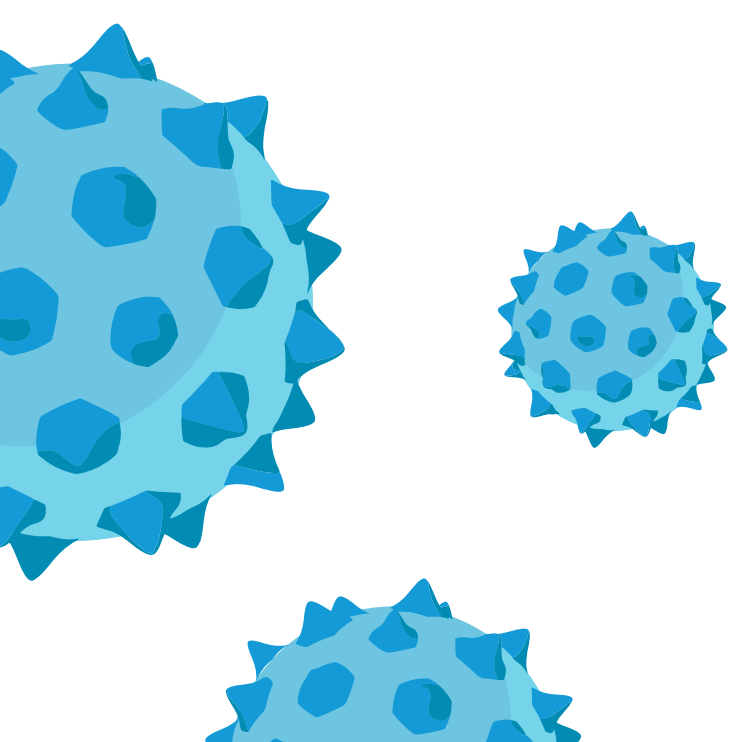
- 1 Test remote log-in capabilities**

Not only should personal devices be configured for secure remote working, but business should ensure that multi-factor authentication (MFA) is set up immediately. MFA is an authentication process that requires more than just a password to protect an email account or digital identity and is used to ensure that a person is who they say they are by requiring a minimum of two pieces of unique data that corroborates their identity. Implementing this significantly reduces the chances of cybercriminals being able to log into a business's RDP. For more information on MFA and how to implement it, [click here](#).
- 2 Train your employees on how to spot a phishing email**

As a CFC cyber policyholder, you can get free access to a range of risk management tools, including CyberRiskAware, an e-learning tool focusing on phishing attacks. This valuable tool teaches people within your business to be more vigilant when it comes to opening attachments, clicking on links, transferring money, or sending sensitive information. To find out more about it, including instructions on how to access it, [click here](#).
- 3 Prepare for operational disruption in advance**

Put simply, prepare for the worst. As with so many cyber incidents, time is of the essence so ensure you have an incident response plan in place, [a template for which you can access for free](#) as a CFC cyber policyholder. And as ever, if you believe that one of your employees has fallen victim or that you are experiencing any kind of cyber event, [notify CFC](#) as soon as possible so that we can help you.
- 4 Finally, be vigilant**

What's becoming clear as this pandemic plays out is that cybercriminals are shifting tactics daily. If you see something on social media or receive an unsolicited email that seems too good to be true, it probably is. Aside from learning how to spot phishing emails, make sure to do your research, use reputable companies, and follow-up requests for money or information with a phone call using a number from a separate, trusted source.



Austin Hepburn
410.901.0735
Austin_Hepburn@RPSins.com