Partners Group
REALIZING POTENTIAL IN PRIVATE MARKETS

How to stay cyber safe during a global pandemic

Q&A with Patrik Bless

Patrik Bless, Chief Information Security Officer

One of the side-effects of the COVID-19 global health crisis has been a large spike in online criminal activity. Cyber attackers are using every conceivable strategy to take advantage of the crisis, from fake Coronavirus cures and ransomware attacks on vaccine test centers to attacks on the World Health Organization itself. We spoke to Patrik Bless, Partners Group's Chief Information Security Officer, to understand what the risks are and how businesses and private individuals can continue to protect themselves against them.

What are the key online risks related to the COVID-19 health crisis?

For private individuals, the main issue is scams, usually delivered via social engineering techniques such as phishing emails. We are seeing scams of all sorts, ranging from requests for money, to fake COVID-19 tracking apps, to the sale of fraudulent in-demand products like face masks and hand sanitizers. For businesses, many of the risks have emerged as a result of them having to hastily implement new protocols and services as a large portion of their workforce moved to a work-from-home set-up. Many companies that did not have the right infrastructure had to allow unauthenticated devices onto their networks or provide access via weak forms of user authentication, making themselves more vulnerable to the risk of data leaks and cyber attacks.

Who is being targeted?

During this crisis, anyone operating under pressure is being targeted. Unfortunately, this means that essential workers and institutions, such as healthcare providers and hospitals, have been at the center of a number of attacks. The same goes for companies that have had to quickly move people out of offices and any form of critical infrastructure. But it is also across the board; anything that can be attacked is being targeted.

> *"It is easy for cyber criminals to leverage the urgency aspect of a crisis like this and the mere distraction it causes for many individuals and businesses."*

Why is this particular crisis being leveraged so much by cyber criminals?

On the one hand, and especially at the beginning, it is easy for cyber criminals to leverage the urgency aspect of a crisis like this and the mere distraction it causes for many individuals and businesses. The fact that there is so much going on and so much noise generated by the crisis makes it hard for people to keep their guard up on all fronts at all times.

On the other hand, cyber criminals are leveraging our increased appetite for information. The crisis has caused a huge demand for information, as evidenced by the fact that many major news outlets are providing dedicated Coronavirus reporting for free. Private individuals in particular are likely to see more attempts from attackers trying to exploit this demand.

As we gradually move into the re-opening phase, fake COVID-19 contact tracing apps could be one example. With a lot of initiatives to trace Coronavirus cases currently underway, there will also be malicious users disguising malware as tracing apps in order to steal sensitive data such as banking details.

What are the key measures businesses can take to protect themselves?

At the start of the crisis, we shared best practice guidelines with our portfolio companies for implementing an immediate response to the crisis and managing remote working set-ups. Our main advice was to avoid jeopardizing policy over pragmatism.

If you need to cross a river quickly, you just build a bridge, without thinking too much about railings or other safety measures. However, without railings, some people may eventually fall into the water. Companies that had to quickly implement work-from-home capabilities they did not have before are in a similar situation: if you do not have much time, you typically just get things up and running and may cut a few corners.

But the reality is that an adequately designed security policy should protect a firm from incidents. That is why understanding the reasons for having had certain measures in place before the crisis started is crucial. For example, if a regulator required you to have certain restrictions on your devices, those requirements will still be there once the crisis is over. Similarly, if you experience a large data breach because of a protocol you broke for the sake of being pragmatic and quick, the resulting damage will not go away once the virus does.

Now that many companies have been operating under these new regimes for some time and as many countries are starting to enter the re-opening phase, it is all about maintaining resilience and also preparing for potential future waves of the virus. During this transition phase, it is important for businesses to keep their guard up and continue to drive awareness among staff, while also preparing their infrastructure for a return to the office set-up.

> *"If you experience a large data breach because of a protocol you broke for the sake of being pragmatic and quick, the resulting damage will not go away once the virus does."*

What measures can we take as private individuals?

For private individuals, not much has changed. It is all about being extra careful when confronted with anything that seems unusual or that is suddenly urgent. While social distancing and home office regimes have actually removed some of the surveillance-related cyber risks that busy travel schedules can introduce, we are still vulnerable to social engineering attacks.

To mitigate the risk of becoming victims of malicious apps or online scams, it is also important to only use trustworthy sources of information on personal devices. The same goes for virtual interactions such as online meetings, which should be carried out on trustworthy channels. If you are using new tools for some of these online interactions, it is important to understand what they do.

Furthermore, if you download new apps such as a Coronavirus tracking app, you need to understand where it comes from and who the authors are. Is it from a legitimate source or is it just a scam to spy on you?

Finally, the usual advice, such as choosing good passwords, enabling multiple-factor authentication where possible, locking devices when not in use and not forwarding work-related emails to personal accounts, still holds true and should also be applied to any new situation you are facing.