Online fraudsters are now exploiting Coronavirus. Why are emails so at risk?

The cyber risk level has also increased this week on the back of Coronavirus as criminals have launched email phishing attacks to steal private information. The US secret service stated criminals are posing as legitimate medical and health organisations to mass disseminate emails tricking individuals to install malware and gain access to logins.

Temps de lecture : minute

---

16 March 2020

This could subsequently result in business accounts or networks being compromised, data breaches and ransom demands. These fear tactics and phishing methods are well known so what has changed this time?

1. Fear of coronavirus, and wanting more information, can cause us to let our guard down
2. Overload of emails. Due to the urgency of the situation, the new processes and systems being implemented by firms, it is harder to distinguish between what is true to what could be fraud
3. IT departments and systems are under increased pressure to prepare for the crisis
4. Increase use of personal computers for remote access may lead to easier attack
5. The usual desk verification “Does this email look odd to you? Did you receive it too?” Doesn’t work as well from home

Yet in reality, if not coronavirus, criminals will find another reason to send

an email to gather this private information. So what is so wrong with email?

Contingency preparedness letter from the European Central Bank

European Central Bank issues COVID-19 letter

Email has the great benefit that everyone can create one and send to anyone. It has therefore become the principal tool to communicate outside of the secure environment of a company. With the same ease, fraudsters can also create an email account which will appear to be sent from bank, a company or in this case, a health organisation and send to your personal or work email address with a link to open or a document to download. Emails are not secure as they are an open system (anyone can send to anyone) and the identity of neither the sender, nor the receiver is verified. You will no doubt have received a phone call, a SMS text, or WhatsApp message from someone impersonating your bank asking for your details, this is not different.

Advice from the United States Secret Service, Department of Homeland Security

Secret Service Issues COVID-19 Phishing Alert

So how can we prevent this phishing happening?

With email you can’t. Companies may include security measures to check for viruses and malware and train employees to spot phishing attempts, but ultimately, they do not control the end points so the risk will remain. Phishing is not only increasing but is constantly getting more sophisticated. Emails are therefore no longer fit for purpose and companies need to establish secure communication channels between staff and clients where security and privacy is ensured i.e. the identity of each participant can be trusted, the data is encrypted and stored safely. Banks have Bloomberg or Symphony to communicate between each other to meet these requirements. We have built Qwil Messenger for all companies to be able to easily invite their staff, prospects and clients to securely chat and share documents, replacing insecure email and non compliant social chat use in businesses.

Laurent Guyot is Chief Revenue & Financial Officer Qwil Messenger, responsible for managing the company from the strategy, multiple rounds of financing through to the marketing of the secure chat platform Qwil Messenger. Laurent brings extensive experience in these domains as well as a significant network of financial services contacts across Europe built over 15 years in investment banking at Citigroup, UBS and Bank of America Merrill Lynch.

Qwil Messenger is a single chat app for everyone, allowing clients of multiple firms to safely engage with their staff representatives within a branded space, fully controlled and coordinated by each firm. Our extensive APIs enable countless automation possibilities (from automating statements, to crisis management) and integration such as AD and Salesforce.

Article écrit par Laurent Guyot