WERKSMANS
ATTORNEYS

REGULATORY

When darkness comes, evil goes phishing....

25 March 2020 *3 min read*

By Ahmore Burger-Smidt, Head of Data Privacy Practice

Let us not doubt the fact that cybercriminals are looking to exploit the spread of Coronavirus to conduct cyberattacks and drive hacking campaigns.

It has been widely reported that numerous companies are experiencing an increase in phishing attacks.

In many cases, these attacks are in the form of phishing emails containing links or attachments that claim to contain important information about the Coronavirus. Once opened, these phishing emails infect the user's computer with malware that can be used to exploit the "infected victim".

At this point in time employees will work from home and IT-help will only be available remotely. To limit disruptions during lockdown, the question would be how to protect your company.

Therefore, what should you inform your employees? Tell them, they should not open a random email:

- until certain that the sender is genuine;
- not follow any links in such email, or
- reply.

Here are some guidance on spotting phishing emails:

- poor grammar, punctuation and spelling;
- poor design and overall quality not in line with your banks normal email;
- is it addressed to you by name, or does it refer to "valued customer", or "friend", or "colleague"? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam;
- does the email ask you to act urgently? Even if it looks on the face of it like an email from a colleague?
- be suspicious of words like 'you have been a victim of crime, click here immediately'; or
- look at the sender's name and email address. Does it look and sound legitimate, or is it trying to mimic someone you know?

Since there is no way to completely protect companies against malware infection, companies should adopt a defence approach. This means using more than one basic approach as defence. This will allow for more opportunities to detect malware, and then stop it before it causes real harm to the company. One should assume that some malware will infiltrate the company, so companies can take steps to limit the impact this would cause, and speed up their response. Your IT department should:

- prepare backups;
- take steps to prevent malware from being delivered to employees working from home;
- take steps to prevent malware from running on company devices; and

- have in place a plan to limit the impact of infection and enable rapid response.

From prevention to recovery

While prevention is generally accepted to be better than the cure, the reality is that prevention of phishing attacks may not be possible. Working under the assumption that a breach will occur and that a phishing attack will succeed at some point, it is imperative that companies ensure they are able to resume normal operations as quickly as possible. Being prepared for an attack and having a well-designed breach plan in place is non-negotiable and should form part of good governance.

There are certain activities which will have to take place during and immediately after a successful phishing incident that should be included in a cyber breach plan. These activities include:

- determining the extent of an incident against the company's systems;
- managing its immediate impact;
- providing advice and assistance to rectify the compromise; and
- working to increase security across the network

Do not allow your company to be in the dark. Keep evil at bay!

Be prepared and keep on doing business.

Ahmore Burger-Smidt

Head of Regulatory

View Profile