COVID-19 - Reported Coronavirus-Related Scams

Whilst we all, businesses and individuals, are preoccupied with managing the impact the Coronavirus pandemic is having on our lives (us, families and employees) sadly there are others who see this as an opportunity to act less honourably.

Concern about the spread of the Coronavirus has triggered the largest "work from home" mobilisation ever seen. Everyone, businesses and individuals need to take care to ensure they remain cyber resilient amid the crisis.

To prevent risk to your businesses systems please:-

Defend against the phishing attach
Researchers have already observed phishing emails posing as alerts regarding the Coronavirus, typically including attachments offering information about the outbreak or advice on how to stay safe. In a climate where everyone is scared and hungry for information best practices can easily be overlooked.

We would ask that all businesses remind their employees of the need to remain vigilant. If in doubt do not open the email. Beware of opening emails on mobile devices.

At Beever and Struthers we run simulated spear phishing campaigns at regular periods during the year, serving as both a reminder to our colleagues of the importance of this area, but also to demonstrate our resilience to any such, real, attack. Clearly up-to-date antivirus and monitoring tools should also be put in place.

Prepare for attack
Whilst all the measures possible can be put in place the sad reality is that threats to the businesses network will occur.

When everyone is working in an office environment that threat, when detected, can be quarantined (a sensitive word at the moment), the compromised computer disconnected from the network while the investigations are undertaken.

When everyone is working remotely businesses should ensure that everyone knows how to contact their IT colleagues immediately. This means a layer of contact that goes above and beyond the typical helpdesk "critical" request.

Although slightly bolting the stable door after the proverbial horse has bolted, businesses should check that they have a robust cyber insurance policy in place that will provide cover for business interruption losses as well as the costs of engaging experts to investigate and repair any breach.

Don't get caught out

- Scammers want to steal your money or your personal information. They do this by calling unannounced at your door, phoning, texting or emailing. They will also advertise on social media.
- The only test available is through the NHS - you cannot buy a test kit or pay for a test from anybody else.
- There is no vaccine or cure.
- Only buy from companies that you have dealt with before and type in their online address if you want to order - don't respond to a link in an email or find them by an internet search because scam sites may be imitating as a genuine company.
- Charities must be registered with the Charity Commission - check they are legitimate before you donate.

COVID-19 - Reported Coronavirus-Related Scams

These current scams are circulating here and abroad:

- Emails pretending to be from the World Health Organisation (WHO) with attachments on how to stay safe - the attachments contain malware which will infect your computer, steal your information and request a ransom.
- Scammers have circulated fake maps via email which claim to show how the virus outbreaks, but, again, they are malware.
- Fake charities asking for donations to help with the coronavirus.
- Fake emails pretending to be from a government department, watch out for websites not ending with “gov.uk”.
- Scammers pretending to be from the UK government, advising that a new tax refund programme has been introduced to deal with the coronavirus outbreak and that you are due a refund.
- Companies phoning to offer to clean and sanitise homes, pre-payment is required over the phone or with gift cards.
- Companies claiming to have or to be on the verge of producing a vaccine and requiring payment to reserve a batch.
- Scammers offering fake investment opportunities in companies working to produce a vaccine.
- Doorstep callers 'checking for coronavirus'.
- Companies selling 'fast COVID-19 tests'.
- Companies selling products that they claim can treat, cure or prevent the virus including face masks.
- Companies selling fake cleaning products and hand sanitisers.
- Websites purporting to offer support in accessing financial support measures.
- Emails suggesting they are from the HMRC.

As always if you want more information, or if we can help in any other way, please get in touch.