East Midlands Special Operations Unit

COVID-19 CYBER PROTECT MESSAGES

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team E: EMSOU-Cyset@leicestershire.pnn.police.uk or your local Force protect team.

Phishing emails/Fraud/Ransomware

Action Fraud has received over 1,000 reports of coronavirus-themed phishing attempts. People are being duped into opening attachments, which then compromise their personal information, email logins, passwords and banking details.

Some of the tactics being used by fraudsters in phishing emails include:

- Purporting to be from the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO) and offering to provide a list of active infections in specific areas. Corrupt links will take victims to a credential-stealing page or makes involuntary payments into a Bitcoin account.
- Publishing misleading articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.
- Sending investment and trading advice to take advantage of the coronavirus downturn.

What to look out for:

- Many phishing emails have poor grammar, punctuation and spelling.
- Poor design and overall quality.
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? Are the latter generic ones, the scammer?
- Asking you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Does the sender sound legitimate? Or trying to mimic someone?
- Sound too good to be true? It probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet.
- Your bank, or any other official source, should never ask you to supply personal information from an email.
- If unsure, check any claims made in the email through some other channel.

Wider fraud

The NFIB (National Fraud Investigation Bureau) has suggested, that the following fraud types could increase during the COVID-19 outbreak:

- Online shopping and auction fraud
- Computer software service fraud
- Lender loan fraud – people look to quick loans to see them through tough times
- Mandate fraud – with more people working from home, it may be easier to impersonate senior decision makers and request a change in direct debit or standing order payments.
- Investment fraud including pension liberation fraud – fraudsters could create bogus investments in commodities in high demand, e.g. oxygen or anti-bac gel.

Computer software service fraud

Criminals may cold call you claiming there are problems with your computer and they can help solve them. They often use the names of known and trusted companies such as Microsoft and Apple, they may also use the name of your Broadband provider.

The criminals may ask you to complete a number of actions on your computer, and may even be able to demonstrate an “error”. Then they tell you they need remote access and ask you to download software, this is known as a Remote Access Tool.

This give the criminal complete access to everything on your computer. They can access and copy your data or download malware to monitor what you do in future.

Never give an unsolicited caller remote access to your computer.

Trending

Banking Trojan being disguised as ‘ways to get rid of Coronavirus’, convincing potential victims into downloading malware.

Fake websites masquerading as coronavirus tracking maps. When users visit the fake site, they’re infected with malware designed to capture sensitive information, including logins for banks, email accounts and social media platforms.

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.

To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.