East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Tuesday 7 April 2020

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 EMSOU Protect Team **or your local Force protect team.**

To coincide with a social media campaign from NFIB, today's topic is **'Computer Software Service Scams'.**

Computer software service fraud

From bogus 'computer software tech support' phone calls, to fraudsters asking for credit card information to 'validate your software', there are a number of computer software service scams you need to look out for.

Common scams that use the brand names include:

- Receiving a phone call from 'Microsoft Tech Support' to fix your computer.
- Receiving unsolicited emails with attached security updates.
- Being asked for your credit card information to 'validate your copy of Windows'.
- Being told you have won the 'Microsoft Lottery'.

Computer firms do not send unsolicited emails or make unsolicited phone calls to request personal or financial information, or to fix your computer.

Advise anyone who receives such communication to delete the email or hang up the phone. Anyone who has lost money to a scam like this should **report it to Action Fraud**.

Top tips to avoid Computer Software Service Fraud

- Never install any software, or grant remote access to your computer, from a cold caller.
- Treat unsolicited phone calls with scepticism and never give any personal information.
- Microsoft does not request credit card information to validate copies of Windows and never asks for any personally identifying information, including credit card details.
- The 'Microsoft Lottery' does not exist –so it's not true if you're told you've won.

Further advice available here from Action Fraud.

East Midlands Special Operations Unit

Hot Topic

Who is listening in to your conference/work calls - Alexa, Siri or Google Assistant?

These devices are **ALWAYS** listening and regularly pass recordings back to their hosts, even if only to check they are working. The big 3 - Apple, Amazon and Google - all admitted to employing listeners to “sample” these conversations for voice quality.

Always be mindful of your location and who might be listening!

If you are having a confidential or sensitive conversation move to another room or turn off the smart speaker

Trending

- Scammers are adopting ever more sophisticated methods as the lockdown continues.

- Data has shown that COVID-19–based attacks are much more successful than typical phishing attacks. To increase their success rate, attackers have adopted multi-stage attacks leveraging email, PDF attachments, and trusted SaaS services.

- A spear-phishing campaign is using fears of the COVID-19 pandemic to spread a specific information stealer called LokiBot which steals a variety of credentials, such as stored email passwords. The body of the email contains multiple points about infection control and pretends to address misinformation related to COVID-19. Victims are mainly in the U.S. and EU so far.

  There have been several reports of emails purporting to be from Virgin Media and BT internet IT helpdesk. Both emails use the corona virus as a hook and direct the recipient to a link in order to provide their details.

- A new COVID related scam reported involves calling business owners, purporting to be from Trading Standards and accuse the business of operating illegally during lockdown and risking a fine. The Fraudsters then follow up with a second call purporting to be from HMRC, issuing a fine and a link on WhatsApp to pay the fine.

- Suspicious callers are said to have been knocking on doors of elderly and vulnerable residents in various parts of the UK, saying that they are health officials doing door-to-door testing.

Reporting

Reporting is CRUCIAL. Please report all Fraud and Cybercrime to Action Fraud either online at or by calling 0300 123 2040.