East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Tuesday 28 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.**

Today's cyber topic is 'ransomware and back ups'

Anyone and everyone who relies on a digital device to create, edit, or otherwise modify data for business and/or personal use should have a backup plan in place to protect that data.

One of the best ways to defend against a ransomware attack is to have a secure back up. With rapid advances in technology from tapes and floppy disks to today's high capacity USB devices, network drives and cloud backups, backing up data is easy. The downside is that these backups are susceptible to infection.

Compare the fortunes of two different organisations we recently worked with. One failed to isolate backups and scan data as it was being written to mass storage and never tested the back up. The other kept their backups separate, regularly scanned them and checked files could be reinstalled.

The first organisation lost over two years' worth of data and took a full month to recover after a ransomware attack. The second organisation was back up and running in less than an hour with no loss of data after a ransomware attack.

A good back up can give peace of mind to personal and corporate users and our top tips for peace of mind are below:

Identify your critical data - For individuals that could include documents, photos, emails, contacts, and calendar information. For a business that would be data that it couldn't function without.

Restrict access and disconnect - Whether on a USB stick, a separate drive or computer, access to backups should be restricted and not permanently connected, either physically or over a network, to the original device copy.

Store backups safely - Consider storing backups in a separate location, so fire or theft won't result in total loss. Cloud storage solutions may be a cost-effective and efficient way of achieving this. Unless running your own email server, emails are already stored 'in the cloud'.

Cloud security guidance - Not all Cloud providers are the same, but most have good security practices. To help when choosing a cloud provider read the NCSC's Cloud Security Guidance.

Make backing up part of your regular routine - The majority of network or cloud storage solutions now allow automatic backups. Using automated backups saves time and ensures the latest version of files is backed up.

When choosing a solution, consider how much data needs to be backed up, and how quickly the data needs to be accessed following any incident

East Midlands Special Operations Unit

Test your backups - You only find out how good your insurance cover is when you make a claim. Data recovery can be a stressful scenario that doesn't need the additional pressure of worrying whether backups are valid or not. The solution is to test that backups have worked by restoring data.

How often should testing be performed? In an ideal world, testing after every backup to validate the data. This is not always practical, a trade-off needs to be made between the impact and effort of recovery and having a degree of confidence in the restore.

Hot topics

Criminals will use every opportunity they can to defraud innocent people. They will continue to exploit every angle of this national crisis.

Phishing emails claiming to be from TV Licensing, referencing the pandemic *'We're sorry but due to the impact of Coronavirus you will need to pay online'* are being reported.

Emails spoofing the HMRC brand asks recipients to send copies of their passport and utility bill/bank statement via a link to an infected site and another variant instructing business recipients to click on a link to complete a claim on the Coronavirus Job Retention Scheme.

There have also been emails where offenders are selling or giving away thermometers, immunity oils, shipping or selling COVID-19 testing kits and emergency medical and survival kits at a reduced rate.

Scammers have also been disguising themselves as representatives of the World Health Organization (WHO), asking for charitable donations. An email asks recipients to use the Bitcoin Network and donate to their wallet address to help *"prevent, detect, and respond to the pandemic".*

A new phishing email purporting to be from PayPal. The email is convincing and is personalised to the recipient. The email contains corporate messaging in relation to the corona virus at the bottom of the email.

Bank customers targeted with a new phishing email containing a link and purporting to be from HSBC. The email claims to be providing all customers with £500 due to the pandemic.

Webinar - Thursday 30th April 2020 @ 1400 – 1500 hrs

This week's topic: **Online fraud…Evolution or Repetition?**

City of London Police's Cyber Griffin team take a closer look at online fraud. The panel of experts will be taking your questions and answering the following:

- Why is online fraud so prevalent?
- Are criminals using new and unique methods, or just repackaging age old techniques?
- How can people and organisations avoid becoming victims?
- What does the future of online fraud look like?

To register for this event click on the following link - places are limited.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.