East Midlands Special Operations Unit

COVID-19 PROTECT MESSAGES

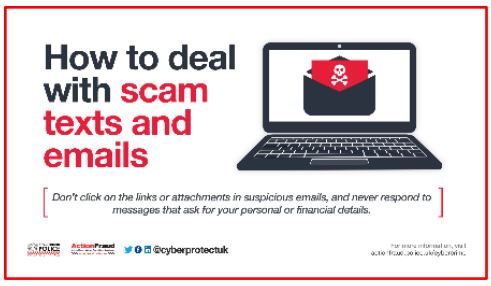
Monday 6 April 2020

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 **'how to deal with scam texts and emails'** - a problem that plagues all users of email and digital devices.



Criminals convince you to click on links in a scam email or text message, or to give information away. Once clicked, you may be sent to a dodgy website which could download malware onto the computer or steal passwords. Given the current coronavirus (COVID-19) situation, criminals are sending emails and texts that claim a 'cure' for the virus, offer a financial reward, or encourage you to donate.

These scam messages can be very hard to spot, and designed to get you to react without thinking. If you think you've clicked on a bad link, don't panic - there's lots you can do to limit any harm. If you've already clicked a link (or entered details into a website), take the following steps:

- If using a work laptop or phone, contact your IT department and let them know.
- If you've been tricked into providing banking details, contact your bank.
- If your account has already been hacked, or you have been locked out of your account, refer to NCSC guidance on recovering a hacked account.
- Open your antivirus (AV) software, and run a full scan to clean up any problems it finds.
- If you provided a password, change passwords on all accounts that use the same one.
- If you've lost money, tell your bank and report it as a crime to Action Fraud.

Top tips for spotting Scam texts and Emails:

- **Authority** - Sender claims to be someone official (Bank, Doctor, Gov department)?
- **Urgency** - You have a limited time to respond?
- **Emotion** - Does the message make you panic, be fearful, hopeful or curious?
- **Scarcity** - Offering something in short supply?
- **Current events** - Current news, big events or specific times of year (like tax reporting).

East Midlands Special Operations Unit

Make yourself a harder target

Criminals use publicly available information to make messages more convincing. Often gleaned from your 'digital footprint' (websites, social media accounts etc). To make yourself less likely to receive phishing emails follow the following advice:

- For social media applications and other online accounts, review the privacy settings.
- Think about what you post, and who can see it.
- Be aware what your friends, family and colleagues say about you online, this can reveal information that can be used to target you.
- If you do spot a suspicious email, flag it as Spam/Junk in your email inbox.

Trending

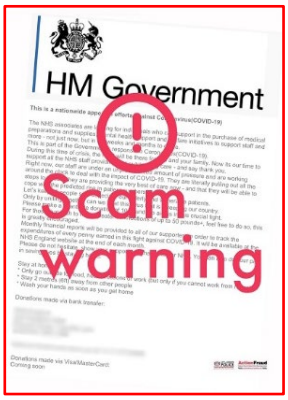
A variation has been seen in the HMRC phishing email scam in which individuals are asked to complete a “coronavirus relief form” in order to receive payment within 2 days.

A spoofing campaign which uses socially engineered emails promising access to important information about cases of COVID-19 in the receiver’s local area is managing to circumnavigate Proofpoint and Microsoft Office 356 Advanced Threat Protections.

Report received of a cyber-attack on a business in which the computers had remote access enabled, which made the network more vulnerable. The attack shut off each computers anti-virus software, then infected the computer with ransomware

NHS Alert

We have received reports of a scam email purporting to be from HM Government asking for donations to the NHS during the COVID-19 outbreak.



This is a fake email and your money will only end up in the hands of a criminal.

The NHS will never ask you to send money directly to a bank account. If you would like to donate to the NHS you can do so via their official channels or your local NHS Trust.

Local

Some parents in Derby have received ‘free school meal’ email, stating the following: *‘As schools will be closing, if you’re entitled to free school meals, please send your bank details and we’ll make sure you’re supported’.*

Official response from GOV.UK here – “We can confirm that this is a scam email and is not official. We urge parents that if you receive any emails like this, please do not respond, and delete it immediately.”

Reporting

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