East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 27th August 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 topic is: Email Security

For many organisations there is a genuine concern that a malicious threat actor will send emails to others, making it seem that the organisation has sent them. This form of attack - known as 'spoofing' - is a concern because individuals and organisations the company does business with, will think the emails are genuine. This makes it easier for criminals to commit fraud, compromising the confidentiality and integrity of the communications. Dealing with the aftermath and reputational harm is both expensive and time consuming.

Good email security involves:

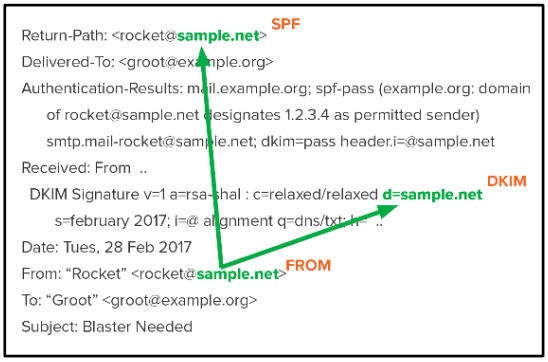
Sender Policy Framework (SPF)
SPF is an email authentication technique, which maintains a list of authorised mail servers. These mail servers are the official point of origin of email communications from an organisation. When the recipient receives an email, the SPF record is used to check that the email originated from an authorised mail server.

DomainKeys Identified Mail (DKIM)

The DKIM is part of a process that lets you 'sign' an email, even ones that you forward. This 'digital signature', is used to prove that the email address was not 'faked' or 'altered'.

Domain-based Messaging Authentication Reporting & Conformance (DMARC)

DMARC brings together the SPF and DKIM mechanisms into a single framework. DMARC will inspect the 'from header' to see if the address shown by the SPF and the address shown in the DKIM signature match. The diagram illustrates how these addresses are checked.



A recipient's system can choose to dump, flag or accept an email that fails the authentication process. DMARC allows the sender to create a policy which can be used to help a receiving system decide what to do in these circumstances.

Copies of messages which fail authentication, will be sent to the purported sender organisation. This will help the organisation fix authentication issues and identify malicious threat actors and web sites.

Encrypting the Entire Message.
Mail servers should enforce strong cryptographic protocols. Cryptography will scramble a message so that any unauthorised party between point A and B, is unable to read an intercepted message. Consult NSCS guidance for configuration details here.

Next Steps
There are a number of open source and commercial tools available which will help an organisation to check the configuration of DMARC, SPF, DKIM. If errors are detected, they often give advice on how to correct the configurations. NSCS recommend the following tools to assess your email security and anti-spoofing measures.

Finally, if you are a public sector body, or an operator of Critical National Infrastructure (CNI) you may be able to sign up for the NCSC's Mail Check service here. Mail Check helps you to setup and maintain good DMARC, SPF, DKIM and email cryptographic configurations.

Hot Topic: Top 10 COVID-19 and lock down frauds, identified by Finance UK

- Fake government emails offering grants
- COVID-19 relief funds
- Council Tax reduction emails
- Universal application help
- Fake NHS Test and Trace
- Fake adverts for COVID related products
- TV Licensing fake emails and texts
- Online TV subscriptions fake update emails
- Fake profiles on social media for online dating
- Social media advertising fake investment opportunities (Bitcoin etc.)

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.
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).