East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 22 June 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: cyber security myths

In an era of misinformation, misleading stories deliberately and inadvertently circulated adding to uncertainty we need to address some of the myths about cyber security.

A lack of information, inaccurate assumptions or inappropriate generalisation are the main causes of security myths.

Myths need to be dispelled, lest we become lax about security and fail to anticipate cyber incidents. Let us explore some of the most common heard today in cyber security.

Myth: *'There is nothing on my computer system that is of any interest to an attacker...'*
Fact: A compromised computer can be:

- Co-opted with bot software to attack other organizations.
- Turned into a file/web server to host illicit or illegal content, such as child pornography.
- Used to capture audio from a mic or footage from a webcam for extortion or blackmail.
- Harvested as a source of email addresses, which can be used for further phishing attacks or other email-based fraud and scams.
- Used to generate cryptocurrency.
- Commit identity fraud or steal services such as Netflix.

Myth: 'Cloud computing transfers the data security risk to the cloud provider…'
Fact: There is no transfer of liability.

If an organisation uses cloud services and suffers a **data breach,** then under GDPR, it is the organisation and not the cloud vendor who are deemed responsible. The concept of 'Due Diligence' is important and the customer must ensure that the services provided by the vendor are fit for purpose and secure.

Myth: Cloud computing offers a secure IT environment
Fact: Do not assume that the Cloud service is inherently secure.

Hosting services in the cloud poses any number of important security risks that must be identified and properly evaluated by the customer. For example, most cloud providers make available a pool of resources to multiple tenants, where the risk of data leakage, can be much greater than in a traditional data centre. Access to cloud resources is often device agnostic, and employees may use personal devices to access data - putting organisation systems and information at risk.

Myth: ‘Anti-virus is the most important method of preventing a cyber-attack.’
Fact: Anti-virus software alone does not guarantee security.

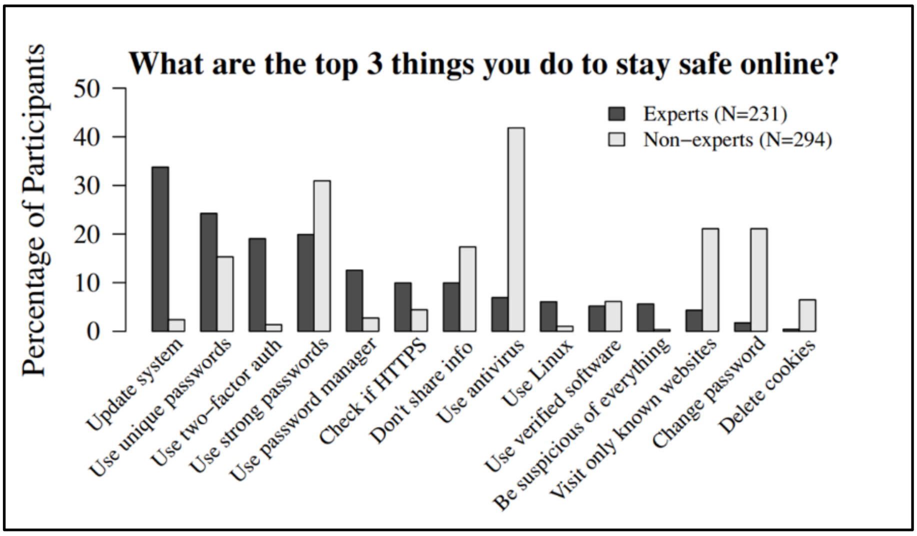
Instead they must form part of a more holistic approach that seeks defence in depth. Network segregation and strong account authentication prevent the spread of any infection and auditing capabilities detect the issue. Staff training is also part of the defence in depth.

Myth: ‘I’d know straight away if my business was compromised.’
Fact: The average time an adversary spends in a network, before detection, is six months.

Attackers will ‘live off the land’ using inbuilt tools security tools, rather than ‘noisy’ exploits; scoping network access and valuable resources. Data might be exfiltrated in drip-feed fashion and security logs cleansed to avoid detection or plant false flags. This is another reason why multiple security controls are preferable to a single solution.

Expert vs non-expert opinion

The survey graph below illustrates the cyber professional’s security priorities versus those of non-cyber professionals.



Graph from: ***https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf***

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).