Eastern Region Special Operations Unit

Regional Organised Crime Unit

# COVID-19 CYBER & FRAUD PROTECT MESSAGES

**Thursday 14th May 2020**

Today's topic is 'Data Breach: Mitigation and Prevention'.

Seldom does a week go by without a major data breach being reported, the damage can be devastating. In the UK the average cost of a data breach has grown to over £2.5 million (IBM research) and the reputational harm can be incalculable.

A data breach is a security incident in which information is accessed without authorisation. In the last few years millions of personal details have been stolen. Organisations targeted and breached include; British Airways, Yahoo, Facebook, Dixons Carphone, Wonga, Ticketmaster, Marriot Hotels, Mumsnet, eBay, Equifax and Travelex.

**Information involved in a data breach usually consists of:**

- Sensitive business data: Information that could impact the reputation or profitability.
- Financial information: Customer bank details, debit or credit card information.
- Personally Identifiable Information (PII): Examples include full name, National Insurance number, bank account number or email address.
- Protected Health Information (PHI): Medical information that identifies an individual.

**How to respond to a breach:**

- Determine the scale of the breach: What data and how many records were compromised.
- How was the data exposed: Trace the path of the attacker, did they move from one system to another? Police cybercrime units can offer expert advice - ask for support.
- Document everything: Who, what, when and why is needed for external agencies but, committing pen to paper will also identify the next logical steps and support a response to future incidents by identifying the appropriate corrective actions.
- Isolate compromised systems: Once isolated, attempt to sanitise them. If an application vulnerability is being exploited, take the application offline. If a malicious insider has leaked information, cut off their access to the organisation's network.
- Instigate business continuity plan. Determine what critical processes must take place and the data these processes need. Have work-arounds been planned out in advance?
- Never underestimate how long an attacker has been entrenched in your systems and what damage may be done.
- Never log into an infected machine with administrative credentials or plug in your backup.

**Communication**

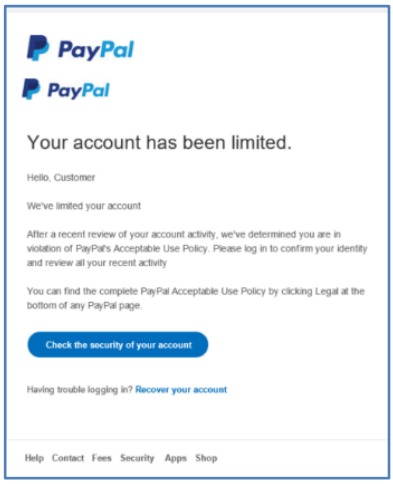
- Breaches need to be reported to the Information Commissioner's Office (ICO) and to individuals if they pose a 'high risk'. Risk refers to the possibility of affected individuals facing economic or social damage, such as discrimination, reputational damage or financial losses.
- You must notify the ICO within 72 hours and affected individuals without 'undue delay'.
- If a crime has been committed, contact Action Fraud.

- If your organisation is affected by industry regulations, other 3rd parties might need informing, seek legal advice if in doubt.
- Determine ways for affected individuals, third parties and the media to make contact.

Further information on how to protect data, from the NCSC, can be found on their website.

## Hot Topics

In just over two weeks since the NCSC and police launched the Suspicious Email Reporting Service (SERS), the public has passed more than 160,000 emails, leading to the removal of over 1,400 links to bogus sites.




Fake emails asking recipients to check the security of their PayPal accounts are being seen.

There are reports of a high number of fake emails stating the government are offering 'emergency COVID-19 tax relief'. Recipients are asked to click on a link to get a free evaluation.

Criminals continue to take advantage of the coronavirus pandemic to commit fraud, as a scam involving the purchase of pets, such as puppies and kittens, continues to be reported to Action Fraud.

## Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

**This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution 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 ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.**