A Coordinated Response to Cyber Crime – March 2015

Both the UK Cyber Security Strategy (2011) and the Serious and Organised Crime Strategy (2013) highlighted the need for an end-to-end national-regional-local response to tackling cyber crime. The range of organisations (set out below) supporting this week of activity co-ordinated by the National Cyber Crime Unit, which focuses on cleaning up malware from known infected servers and raising awareness of the simple steps the public can take to protect themselves, demonstrates how the integrated law enforcement response is working well to respond to the range of cyber crime threats affecting individuals and businesses.

The key organisations in this campaign are:

Victims of cyber crime – how the public and businesses should report cyber crime

Action Fraud – the one stop shop for reporting Cyber Crime

Action Fraud is the UK's national fraud and cyber crime reporting centre, providing a central point of contact for citizens and businesses. The National Fraud Intelligence Bureau, also hosted by the City of London Police, acts upon the information and crimes reported to Action Fraud, developing and disseminating crime packages for investigation locally, regionally and nationally, and executing a range of disruption and crime prevention techniques for victims across all sectors to target criminality and engineer out the threat from fraud and cyber crime.

You can report fraud and cyber crime to Action Fraud online at www.actionfraud.police.uk or by speaking to a specialist fraud and cyber crime adviser on 0300 123 2040.

You can find the latest information on how to protect yourself from fraud and cyber crime at www.facebook.com/actionfraud or on Twitter @actionfrauduk

Cyber security awareness and advice – where the public and businesses can go to get the information they need to protect themselves

Cyber Streetwise

Cyber Streetwise is a cross-government campaign, funded by the National Cyber Security Programme, and delivered in partnership with the private and voluntary sectors. This campaign is led by the Home Office, working closely with the Department for Business, Innovation and Skills and the Cabinet Office.

It aims to measurably and significantly improve the online safety and confidence of individuals and small businesses (SMEs). It encourages people to take responsibility for

their activities online and adopt good basic cyber hygiene such as using strong passwords, installing anti-virus and downloading software security updates.

To learn more about it, and to access resources and information around being Cyber Streetwise, visit www.cyberstreetwise.com

Get Safe Online

Get Safe Online is a leading source of unbiased, factual, and easy-to-understand information on online safety. It is a public/private sector partnership supported by HM Government, as well as leading organisations in banking, retail, internet security and other sectors.

The website is a unique resource providing practical advice on how to protect yourself, your computers and mobile devices, and your business against fraud, identity theft, viruses, and many other online problems. It contains guidance on a range of subjects and topics, from gaming to shopping online, from performing backups to choosing passwords. Alongside the website, it organises Get Safe Online week, and works closely with law enforcement agencies and other bodies in their outreach activities.

To find out more, visit www.getsafeonline.org

CERT-UK

CERT-UK is the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy. Its four main responsibilities are national cyber-security incident management, support to the critical national infrastructure to handle cyber incidents, promoting cyber-security situational awareness across industry, academia and the public sector; and providing the single international point of contact for coordination and collaboration between national CERTs.

The Cyber-security Information Sharing Partnership (CiSP) is a joint industry and government platform that allows members to share cyber threat and vulnerability information in order to increase awareness of issues and therefore reduce the impact on UK business.

Learn more about CERT at https://www.cert.gov.uk/ and https://www.cert.gov.uk/cisp/

The Law Enforcement Response – how the police work together

The National Cyber Crime Unit (NCCU)

The NCCU, part of the National Crime Agency, is the UK's lead for tackling the threat from serious and organised cyber crime. The NCCU leads, supports and coordinates cyber law enforcement activity across the UK, working with partners to provide

specialist cyber support and expertise across law enforcement. It works closely with Regional Cyber Crime Units and Police Forces to build an effective cyber response across the UK.

The NCCU focuses its activities on arresting and disrupting cyber criminals and the infrastructure they use to commit offences. It also looks at innovative ways to prevent people from becoming involved in cyber crime, helping to protect the public from becoming a victim of cyber crime, and ensuring that the UK is prepared and equipped to respond to significant cyber incidents.

Learn more about the work of the NCCU at www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

Regional Cyber Crime Units

Regional Cyber Crime Units (RCCUs) deliver a specialist regional and local cyber investigative capability. They sit within, and are supported by, the wider Regional Organised Crime Unit (ROCU) core capabilities, creating a cohesive response to serious and organised cyber crime across each region. They bring cyber skills to the investigation of serious and organised crime as one of the stable of skills held at ROCU level. They form part of a national response network capable of supporting the NCCU, and work in partnership with the NCCU to arrest cyber criminals and prevent cyber crime.

RCCUs increase cyber awareness across their local police forces, community safety programmes and criminal justice partners. They create local partnerships with academia and industry in order to develop synergies in cyber capability around prevention of, and response to, cyber incidents. They help regional industry protect itself from cyber crime through the creation and facilitation of regional information sharing partnerships.

Police Forces

Local police forces have the responsibility to investigate cyber crime at a local level. They work closely with Action Fraud to ensure an appropriate police response to reports from the public and businesses. They share their knowledge of the cyber crime threat to improve the regional and national picture, and support cyber crime operations led by regional and national teams. Forces are also responsible for supporting their local communities to be better protected from cyber crime by sharing key messages on how to stay safe online.