PSNI CYBER CRIME CENTRE

INFORMATION SHEET – 15/04/20

This information sheet has been compiled by the Police Service of Northern Ireland Cyber Crime Centre and is intended to raise awareness of current threats and available guidance. Advice and information is changing daily as we all navigate our way through the current COVID19 pandemic so please ensure you only take information from reputable sources.

Dealing with Suspicious Messages and Emails

A new wave of sextortion phishing emails appears to have been launched over the weekend with multiple reports being made locally. Usually caught by spam folders, this current version of an old message has been successfully reaching inboxes. While we have seen slight variations in the sum being sought and various Bitcoin addresses, the emails reported start with the text shown. Advice relating to Sextortion emails can be found here.

As you will no doubt have seen over recent weeks, online criminals have been using COVID19 as a core theme of phishing campaigns be that by email or SMS. These may be designed to capture log on credentials, acquire banking information or as a precursor to ransomware, incidents which have not disappeared because more people are working from home. For current guidance and pdf you can share see: Suspicious Email Actions

> I know, ******, is your password. You don't know me ad you're thinking why you received this email, right?
>
> Well, I actually placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account and email account.

> Hi there!
>
> We have amazing news for you!
>
> Due to the COVID-19 pandemic many of our regular players have to stay home.
>
> In order to support you, we have decided to send you one ticket so that you can participate in the draw for free.
>
> This ticket is assigned to your e-mail address and you can participate in the game as soon as it is activated.
>
> Click on the link to activate your ticket and start the game!
>
> --
>
> You received this email as part of the #StayAtHome international lottery promotion.

Introducing the Little Book of Cyber Scams

In conjunction with ScamwiseNI, the PSNI Cyber Crime Centre is pleased to announce the adoption of 'The Little Book of Cyber Scams' from our partners in the Metropolitan Police Service. Aimed at both individuals and Small & Medium Enterprises, the Little Book of Cyber Scams aims to provide advice on common cyber threats and ways to mitigate risk as well as signposting to local resources such as the NI Cyber Security Centre. If your organisation would be interested in hosting / promoting the online version of this booklet please contact Cyber Protect

NCSC – Weekly Threat Report

This week's Threat Report from the NCSC covers a recent blog post by Rapid7 on the discovery of over 350,000 Microsoft Exchange servers exposed on the internet and not patched against a remote code execution vulnerability subject to a Microsoft patch on February 22nd. Weekly Threat reports from the NCSC can be viewed on the NCSC website or CiSP.

Useful websites
www.actionfraud.police.uk
www.ncsc.gov.uk
www.nicybersecuritycentre.gov.uk

Social Media
@PSNIBelfast
@cyberprotectUK
@ncsc