PSNI CYBER CRIME CENTRE

INFORMATION SHEET – 24/04/20

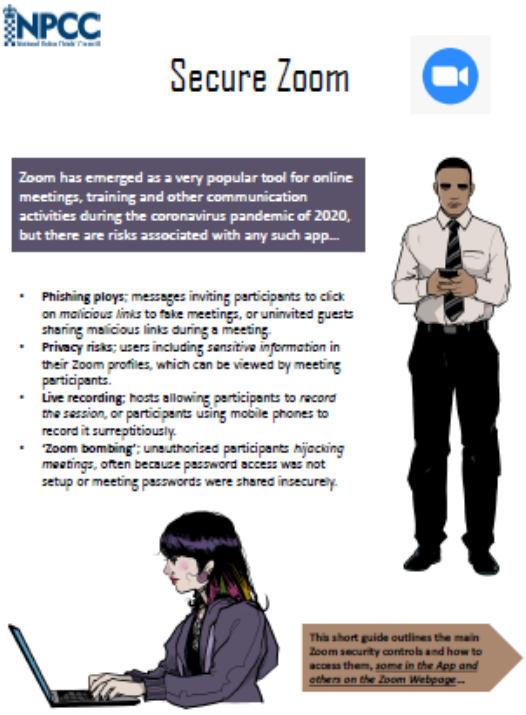
This information sheet has been compiled by the Police Service of Northern Ireland Cyber Crime Centre and is intended to raise awareness of current threats and available guidance. Advice and information is changing daily as we all navigate our way through the current COVID19 pandemic so please ensure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

ZOOM

Alongside recent NCSC Video Conferencing guidance aimed at helping both individuals and organisations with home working, the National Policing DCG Futures Group have released advice on Zoom security controls and how to access them.

With many media channels showcasing the expanded use of ZOOM on the one hand and alleged vulnerabilities and exploitation on the other, we have been introduced to new terms such as 'Zoom Bombing' and many may pause for thought when asked to join a Zoom event.

For most users, joining an meeting should require nothing more than a link and a password but for those setting up Zoom accounts this advisory may be a useful guide alongside advice from the vendor themselves.



Zoom guide is available here:

Coronavirus Scams

The latest figures from Action Fraud show some 1072 victims across the UK have reported coronavirus related scams involving losses of just over £2.3 million alongside 4241 coronavirus related phishing emails. As reflected in local incidents, reports seen include fake websites offering PPE equipment, Facebook ads for non-existent masks and the advertising of suspect home test kits.

If an email reaches your inbox your email provider has not identified it as spam. We would encourage everyone to report suspicious emails to the new NCSC Suspicious Email Reporting Service – report@phishing.gov.uk before marking the email as spam/junk.

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

Social Media
@PSNIBelfast
@cyberawaregv
@ncsc