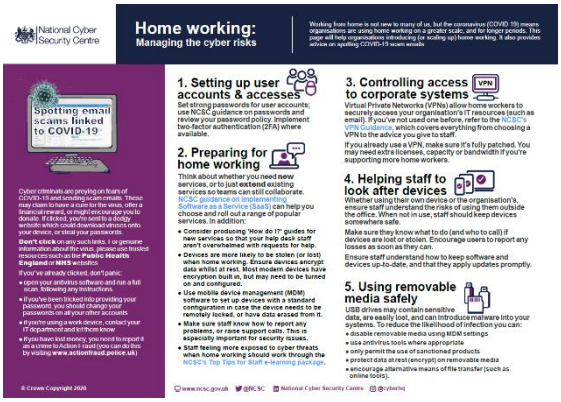
POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

LOCKDOWN REMOTE WORKING GUIDANCE

HOME WORKING As we once again move into lockdown and remote working becoming more prevalent across the business sector we wanted to reiterate the following guidance to ensure a safer cyber secure working environment.



We recommend you read the NCSC guidance to prepare your staff for remote working which is available on the following link. https://www.ncsc.gov.uk/guidance/home-working . This covers the essential recommendations for business to protect their information. A useful infographic is available here https://www.ncsc.gov.uk/files/home%20working%20v1.pdf

USING PERSONAL DEVICES FOR WORK If staff are using their own devices to connect to your network please ensure you are conversant with the NCSC guidance at the following https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device

PHISHING EMAILS During the previous lockdown there was an increase in online cyber related crime. We recommend your staff are aware of the signs of Phishing emails and have the knowledge to recognise and report such emails. Guidance is available at https://www.ncsc.gov.uk/guidance/suspicious-email-actions

STAFF TRAINING It is important that staff understand their roles and responsibilities in regards to Cybercrime prevention and it may be prudent to reaffirm staff training and update security protocols during this period. You can access free staff training and ensure updates are enacted promptly on all devices. The wellbeing of staff is also important at this time and it is incumbent on managers to support staff during the period and ensure any Cyber related concerns are addressed timeously with privileged access levels to confidential information being reviewed as required. Free online staff training is available from the NCSC at the following link;

https://www.ncsc.gov.uk/training/StaySafeOnline_web/index.html#/menu/5f215cc1006d2436a3b6c5e2

BUSINESS EMAIL COMPROMISE (BEC) is a form of phishing attack, typically a cybercriminal will send a fake invoice or request for payment information to be updated. Another tactic is sending an email posing as a manager or CEO within a company.Always be sceptical of urgent and hurried requests to transfer/pay invoices. Verify these requests using known contacts.The National Cyber Security Centre have produced an infographic that outlines this security threat and actions to take to avoid BEC: https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf

VIDEO CONFRENCING As businesses move to a more Cyber resilient footing video conferencing will become more prevalent in everyday work. Guidance on Video Conferencing is available at https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101. For all emergency calls, dial 999.

This alert was sent out for your information by Police Scotland
Cybercrime Harm Prevention Unit - PPCWCyberHarmPrevention@Scotland.pnn.police.uk
All information was correct at time of distribution. 07/01/2021.