NCG

Top Ten Cyber Security Tips when Working from Home

When working remotely it's more important than ever to remember to keep yourself and the NCG systems safe and secure. The rate of Covid related cyber attacks increased by over 450% in one week according Digital Planet.

As a quick reminder of the key points of NCG's Information security guidelines, we have created this guide to help you.

1

Check the address

Always ensure you check the address from which received messages have originated. Recent phishing attacks have been less personalised including requests for donations, offers of cures and investment opportunities. Initial approaches have been in the guise of blackmail, and most concerning, brand impersonation.

Over 32%

of attacks have involved fake Microsoft sign-in portals

Over 20%

have involved those of Apple

Many other fake sites exist including Amazon, LinkedIn, FedEx, UPS and others. E-mails may claim to be "very urgent" to impersonate staff, so again, please be vigilant.

2

Personal Data

Double check the recipient's address when sending communication via Microsoft Outlook or Microsoft Teams containing personal data. If personal data is to be shared consider alternative options such as SharePoint or OneDrive. Personal data is data that can be used to identify a living individual, such as:

✓ Name ✓ Address ✓ Date of birth

3

Message content

Take care when writing e-mails or sending messages via Microsoft Outlook or Teams including the Chat functionality – the contents may be used/requested by the individual concerned or read by others under GDPR rules.

Avoid being subjective and critical of an individual in an e-mail or attachments, or when using the chat functionality. Be objective and factual.

4

Password Protect

Protect documents with a password in order to prevent users from accessing personal data or information that they should not be able to access. When sending a password protected document via email, it is important to remember not to send the password within the email.

This should be given to the recipient via another method e.g. text message, in person or in a separate email.

Alternatively use a more appropriate and secure method to share the data e.g. OneDrive

5

Use NCG Systems

Where possible, staff should ensure any work they do is within NCG systems and not downloaded on their personal devices. Staff should not send business or personal data to their personal e-mail address.

6

Office 365

Work within Office 365 whenever possible. This avoids the need to download documents onto personal devices and can be saved to your Office 365 account.

7

Be protected

When using a personal device, ensure that it is fully updated and protected with the latest anti-virus and anti-malware software.

8

Remove data

In instances where downloading personal data onto your personal device is unavoidable, ensure that once the data is no longer needed it is removed from the device.

9

Keep passwords safe

Ensure that your account passwords are not revealed to others or allow the use of your account, including family and other household members when work is being completed at home.

10

Report breaches

Please report any potential data breaches, as soon as you are aware of them. You can report potential breaches to dpo@ncgrp.co.uk