[SLIDE 5]

What can data controllers do to address and/or reduce the risk of experiencing a phishing attack?

We often receive calls on the personal data breach advice/reporting line from data controllers about phishing attacks and whether they need to report a personal data breach to our office.

It may be helpful to be aware of what steps data controllers can take to address or reduce the risk of experiencing a phishing attack in future as this advice can be provided during the call prior to directing them to report online (if relevant).

A data controller may wish to consider the following:

- **Anti-spoofing controls**

  Anti-spoofing controls stop attackers from spoofing a data controller's domain. They work to confirm the senders identity and tells the recipient's email service what to do with emails that fail the check. The two that organisations should have are DMARC (Domain based message authentication, reporting and conformance) and SPF (Sender Policy Framework) which is a list of the domains or IP addresses used to send emails. DMARC will check the SPF to ensure the sender is legitimate.

- **Reducing information available**

A data controller may wish to review what publicly available information they have as this will make it harder for an attacker to pose as a legitimate source.

- **Filtering/blocking services**

  Filtering services – send emails to spam/junk folders

  Blocking services – block emails to ensure they don't reach the user.

  Data controllers can set up rules to suit their organisation's needs. Techniques for filtering include IP addresses, domain names, white/black listing etc.

- **Training**

  Data controllers should consider carrying out training to help users identify phishing emails (such as using simulations) and training to encourage them users to report any suspected phishing emails they come across. (CPNI's 'Don't Take the Bait!' Campaign also covers this)

  Data controllers can also train staff to check for obvious signs of phishing within emails. For example, poor spelling and/or grammar and low quality versions of company logos.

- **Recognising fraudulent requests**

  Data controllers can make it easier to recognise fraudulent requests by reviewing what processes could be mimicked and how these could be reviewed. (For example, they can ensure email requests are verified by using a second type of communication such as SMS, Phone, logging in etc. They could also consider sending files in a different way such as via an access controlled cloud account).

- **Internal reporting**

  Encouraging a culture of reporting phishing attempts will allow data controllers to take steps to review the technical measures they have in place and improve awareness amongst staff.

- **Malware protection**

  Data controllers should take steps to protect devices from malware. Well configured devices with good end point defences can stop malware installing, even if the email is clicked. For example,

disabling macros, anti-malware software, only using supported software and devices, ensuring devices have up to date patches, and running a proxy service (in house or in the cloud) to block any attempt to reach websites that have been identified as hosting malware or phishing campaigns.

- **Effective authentication and authorisation**

  Effective authentication and authorisation can make the login process more resistant to phishing. These include two-factor authentication/multi-factor authentication, password managers, and alternative login mechanisms such as biometrics. Data controllers can also limit the number of accounts that have privileged access (these should be reviewed regularly) and may wish to ensure staff with privileged access don't browse the web or check emails from an account with administrative privileges. They should ensure they remove/suspend accounts that are no longer being used.

- **Incident response plan**

  Users should know how to report incidents and data controllers should have a plan in place to address any incidents that occur. E.g. forced password reset.

  The NCSC have created 'exercise in a box' which is an online tool that helps organisations establish how resilient they are to cyber-attacks.

- **Support from email service provider**

  Data controllers may wish to consider what measures their own Email Service provider (i.e. Gmail, Office365) supports. For example, most will allow the organisation to disable mail forwarding rules for external email addresses or configure alerts for unusual login activity.