01793 722446
info@haydonwick.gov.uk
www.haydonwick.gov.uk

Haydon Wick Parish Council
Thames Avenue
Haydon Wick
Swindon
SN25 1QQ

Meeting	Full Council
Date	25th October 2022
Report Title	Phishing Email Report
Agenda Reference	11
Author	Laura Cutter, Deputy Clerk & Services Manager

Officer's Recommendation

1) To note the contents of the report.
2) To note the Deputy Clerk & Services Manager is awaiting a response and costs from Orchard regarding the email filtering system as a preventative measure.
3) To note a National Cyber Security Centre document as a training aid to prevent future phishing attacks.

Background/ Purpose

On Monday 10th October 2022 the deputyclerk@haydonwick.gov.uk email address was subject to a phishing email which contained an attachment from a neighbouring Parish Council and a known contact, which the Deputy Clerk & Services Manager coincidentally was awaiting for an email from the contact, and subsequently opened the link. No passwords were requested at the time of opening the email, it may be as the email account was already 'signed in'.

The Deputy Clerk contacted the neighbouring Parish Council who explained the email was not legitimate and after that several emails, similar in content, was sent from the deputyclerk@haydonwick.gov.uk email address.

Due to the email address having been used for several years for resident enquiries and dealing with suppliers, the email was circulated widely, and the office received several phone calls. The IT provider investigated the issue and blocked the deputyclerk@haydonwick.gov.uk email address. An automated email message was set up requesting recipients to delete and disregard the email.

Response from IT Provider

I can see that it has not been spoofed; the mailbox was compromised so it appears as "genuine". The email does contain a phishing link, but you have basic spam filtering via 365 rather than something more robust like Mimecast. Once a phishing link is known, it does take time for other security products to also become aware and update their definitions. It's very likely that Microsoft spam filter simply wasn't aware of this in time.

To resolve the issue, we blocked your account upon receiving the email from yourself, logged off any active sessions on the account then changed the password with you over the phone. We removed the rules set to redirect the email to the deleted folder and removed your email from the spam blocklist.

To avoid this in the future, I would strongly recommend email filtering and implement 2 Factor Authentication for all users. Had your credentials been phished, they would still have to approve the login via a phone app or rolling 6-digit code. If this is something you are interested in, as these types of phishing emails are becoming more common, I can pass this over to the sales team to discuss further.

GDPR
The email account does not store personal information and therefore no private data was compromised. The email addresses were collected from archived files of previous contacts from where the account has been used for several years. The email contacts have been filtered now for only contacts within the last 24 months and will regularly update. A message to the recipients of this nature was sent. This phishing attack was to circulate widely and obtain responses rather than scam people for personal data.

The Deputy Clerk as the Data Protection Officer has reported the incident to the ICO just to ensure that no data has been compromised.

Response from ICO
You should keep an internal record of the breach as detailed in Article 33 (5) of the GDPR, including what happened, the effects of the breach and remedial actions taken.

There is no requirement to notify the ICO, but you should keep a note of why you came to this decision. If new information which affects the circumstances of this breach comes to light, you should reassess the risk and determine whether it becomes reportable at that point.

Internal Training Aids & Next Steps
- Staff & Councillors to be briefed on https://www.ncsc.gov.uk/guidance/phishing
- Those affected have received a response with the information as above
- This report will act as the internal records as per the ICO guidance
- IT provider to give details of the filtering information which will be reported at a future meeting
- All Staff & Councillors responsible for their own housekeeping of email accounts and delete any not used for last 18-24 months.