Phishing Net AI for Microsoft 365

An Outlook Add-In by Sperry Software

The Problem

Gone are the days of obvious recognition of spam emails (think Nigerian prince emails with spelling and grammar mistakes). Today, using AI hackers can be extremely effective at social engineering and can create emails that are very good at making their emails look like it's from another employee at the same company, or someone that can be trusted.

From the NYTimes:
"In many ways, this hack began like any other. The cybercriminals sent their victims infected emails - a news clip or message that appeared to come from a colleague - as bait. When the bank employee clicked on the email, they inadvertently downloaded malicious code."

From Krebs on Security:
“When that email came through, the difference didn’t jump out at me. In hindsight, it blows my mind that it doesn’t bother me more than it did. But in the hustle and bustle of the day, I was not on guard for something like this. Now, I’m second-guessing everything.”

Even worse, Bleeping Computer recently reported on the ‘Greatness’ PaaS, or Phishing as a Service (New 'Greatness' service simplifies Microsoft 365 phishing attacks (bleepingcomputer.com)). You simply provide a list of email addresses and let the ‘Greatness’ service do the rest of the work.

Other vendors’ solutions usually involve training users to look for tell-tale signs like:

- The email being received at an unusual time
- The subject not being relevant to the content in the email
- Attachments that aren’t expected
- Who it’s From, or who else is in the To or CC addresses
- The body of the email has grammar or spelling mistakes

In the past this was a solid way to defend against run of the mill phishing attacks but now using AI all of these items can be improved to the point that it is very difficult for users to discern whether emails are valid or not.

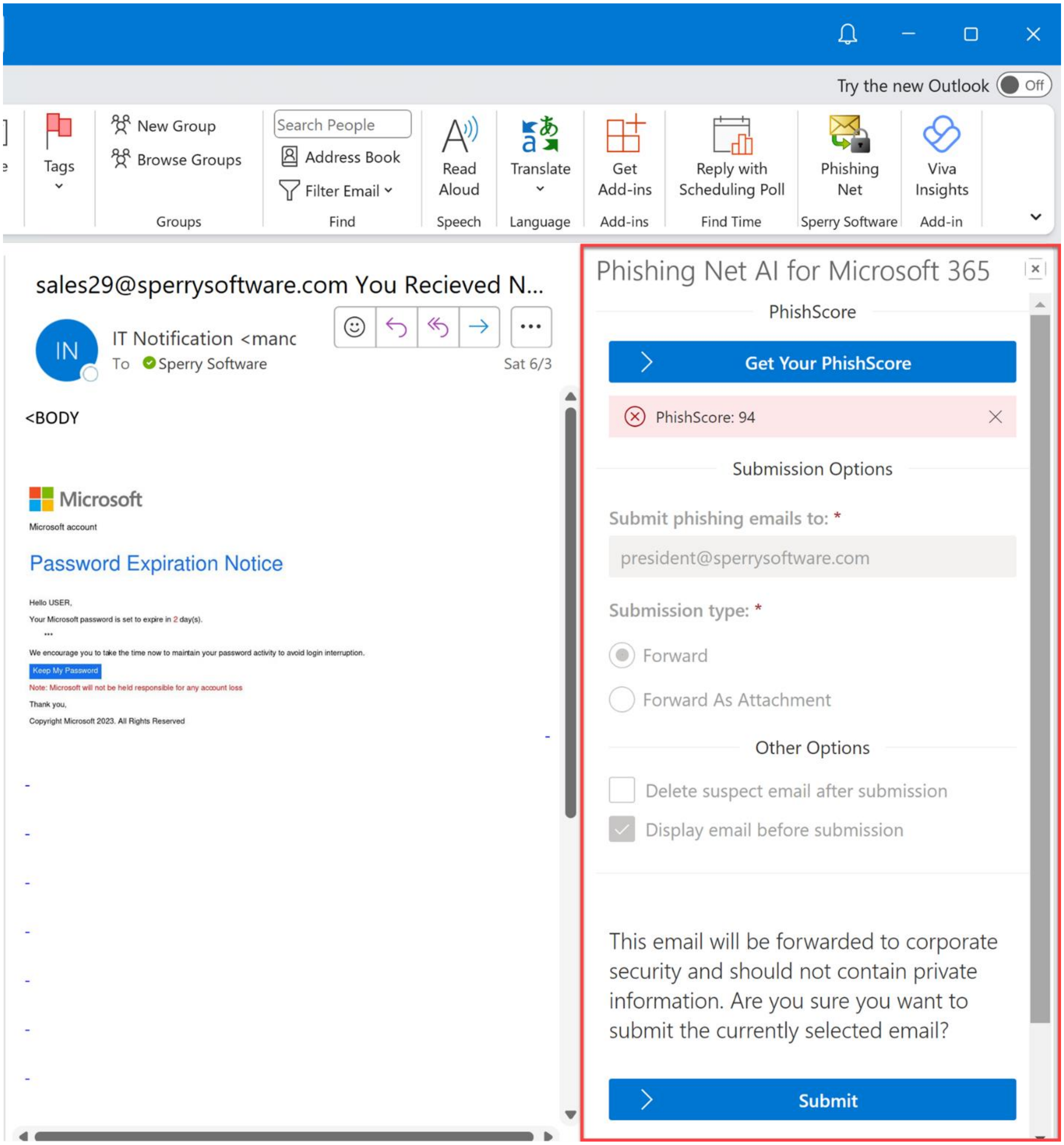
In fact, using AI malicious actors can find details about employees at a particular company through standard social media sites and craft an email asking about pertinent, relevant details that the spear phishing target may have mentioned on LinkedIn, Twitter, or Facebook. This can be about anything – not just business related – anything to get the user to click on a malicious link. Our accompanying whitepaper “Large_Language_Models_Can_Be_Used_In_Phishing_Attacks.pdf”, by Oxford professor Julian Hazell details this process.

The Solution

How will you deal with this threat?

The first thing is begin establishing *layers of defense*. Use Microsoft Defender for Office 365, Exchange Online Protection (EOP), and any other defenses that are available and affordable for you. Continue user training as well, since the older style phishing emails will still continue to get through the cracks and land in your and your user’s Inboxes. Finally, get AI on your side by using a tool like the Phishing Net AI for Microsoft 365.

The Phishing Net AI for Microsoft 365 is an Outlook add-in that uses AI to analyze the email and determine the likelihood that the email is in fact a spear phishing attempt. It works by looking at the one attack vector that hackers need - URLs in the email - and providing a PhishScore™, a composite score representing the likelihood that the email contains malicious links:



sales29@sperrysoftware.com You Recieved N...

IT Notification <manc

To Sperry Software

Sat 6/3

<BODY

Microsoft

Microsoft account

Password Expiration Notice

Hello USER,

Your Microsoft password is set to expire in 2 day(s).

***

We encourage you to take the time now to maintain your password activity to avoid login interruption.

Keep My Password

Note: Microsoft will not be held responsible for any account loss

Thank you,

Copyright Microsoft 2023. All Rights Reserved

Phishing Net AI for Microsoft 365

PhishScore

Get Your PhishScore

PhishScore: 94

Submission Options

Submit phishing emails to: *

president@sperrysoftware.com

Submission type: *

● Forward

○ Forward As Attachment

Other Options

☐ Delete suspect email after submission

☑ Display email before submission

This email will be forwarded to corporate security and should not contain private information. Are you sure you want to submit the currently selected email?

Submit

Once installed, it adds a toolbar button that users can click on to reveal a phish fighting task pane. From here, users can get the PhishScore™ for that email, and can easily submit it if necessary to their corporate security officer (CSO) or relevant security team.

Unlike other services that provide URL validity that can take anywhere from 30 seconds to two minutes to respond, our add-in is designed to respond in just seconds, and it works right in Outlook. An easy to read score instantly lets users know that they are dealing with a dangerous email and also instructs them on the next step (that is, to submit the email to your CSO, and possibly remove the email from their Inbox).

This last part is important because it is necessary to instruct the user what to do once they have determined that the email is in fact a phishing attempt because the problem is that while the users send the phishing email, they may have not attached the phishing email to a "safe" email, and you don't know what they did with the phishing email after they sent it.

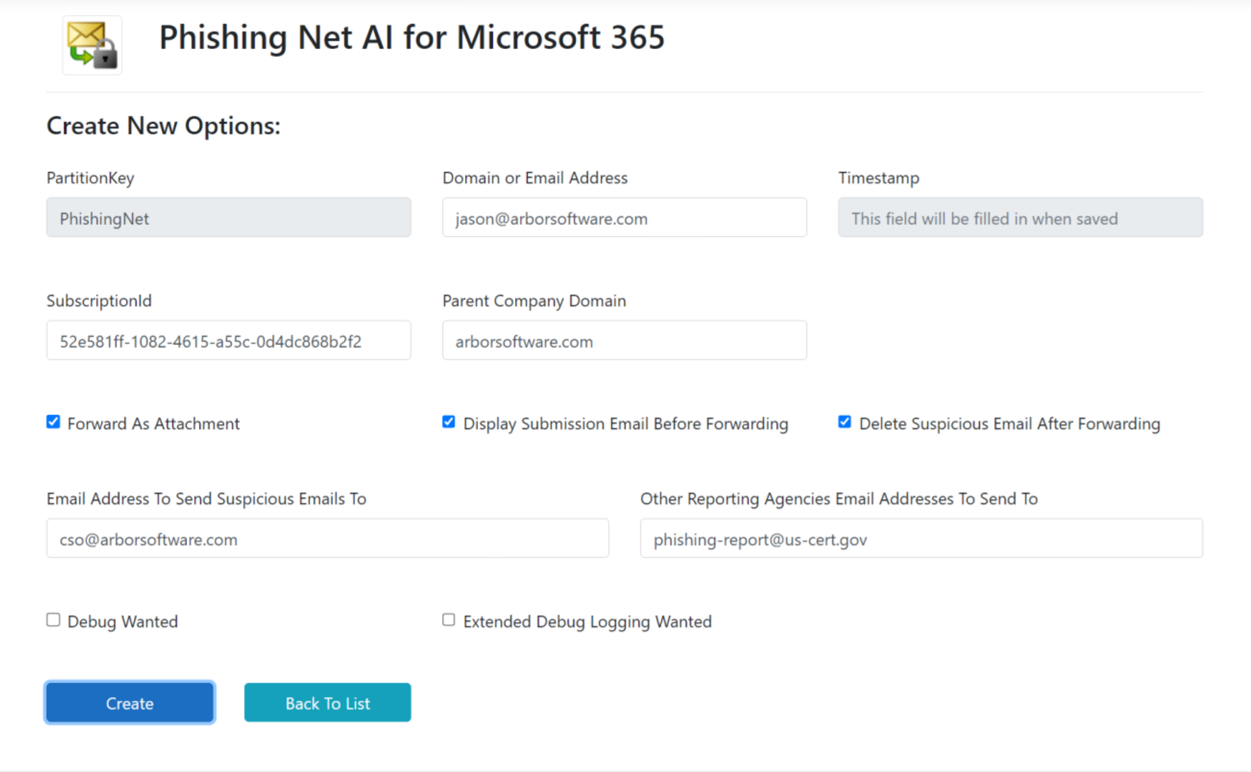
The Phishing Net AI add-in alleviates this by standardizing what to do with the email after it has been identified as being malicious. Administrators can decide to have all users forward the email as an attachment, delete the phishing email from the user’s Inbox, and even report the phishing email to other authorities like the FTC, DHS, or Microsoft’s spam/phish fighting unit.

Finally, the add-in also keeps track of the bad URLs and this information is aggregated across all our customers so that as more and more people use the service, it grows stronger and helps you to identify when a corporate wide attack may be taking place so that you can send an alert to your users to let them know to beware.

This add-in, like many Sperry Software add-ins, was made with the input and suggestions of other Sperry Software customers. We think it will make a great addition to your *layers of email defenses*.

Centralized Control

The Phishing Net for Microsoft 365 add-in is configured through the use of a dashboard. With it, all the options available to configure the add-in (including what to do with an email after it has been identified as a phishing email) can be set for yourself or for all the users in your tenant:



Phishing Net AI for Microsoft 365

Create New Options:

PartitionKey: PhishingNet

Domain or Email Address: jason@arborsoftware.com

Timestamp: This field will be filled in when saved

SubscriptionId: 52e581ff-1082-4615-a55c-0d4dc868b2f2

Parent Company Domain: arborsoftware.com

☑ Forward As Attachment ☑ Display Submission Email Before Forwarding ☑ Delete Suspicious Email After Forwarding

Email Address To Send Suspicious Emails To: cso@arborsoftware.com

Other Reporting Agencies Email Addresses To Send To: phishing-report@us-cert.gov

☐ Debug Wanted ☐ Extended Debug Logging Wanted

Next Steps

1. You can sign up for a free trial or a paid subscription using our listing on Microsoft AppSource.
2. If you prefer direct billing, you may have already received a quote – if not, you can request one by emailing sales@sperrysoftware.com. Be sure to include an estimate of the number of users. If you already have a quote, then getting a purchase order is the next step, unless using a credit card.
3. Once you signup, you can go to your dashboard at https://dashboard.sperrysoftware365.com and begin configuring your settings.
4. Finally, be sure to actually install the add-in into Outlook either for yourself or for your users using the Microsoft Admin Center.