



Security Awareness Training Blog

8

Jul

Scam Of The Week: Microsoft OneNote Audio Note Phishing Emails

 Stu Sjouerman

Tweet



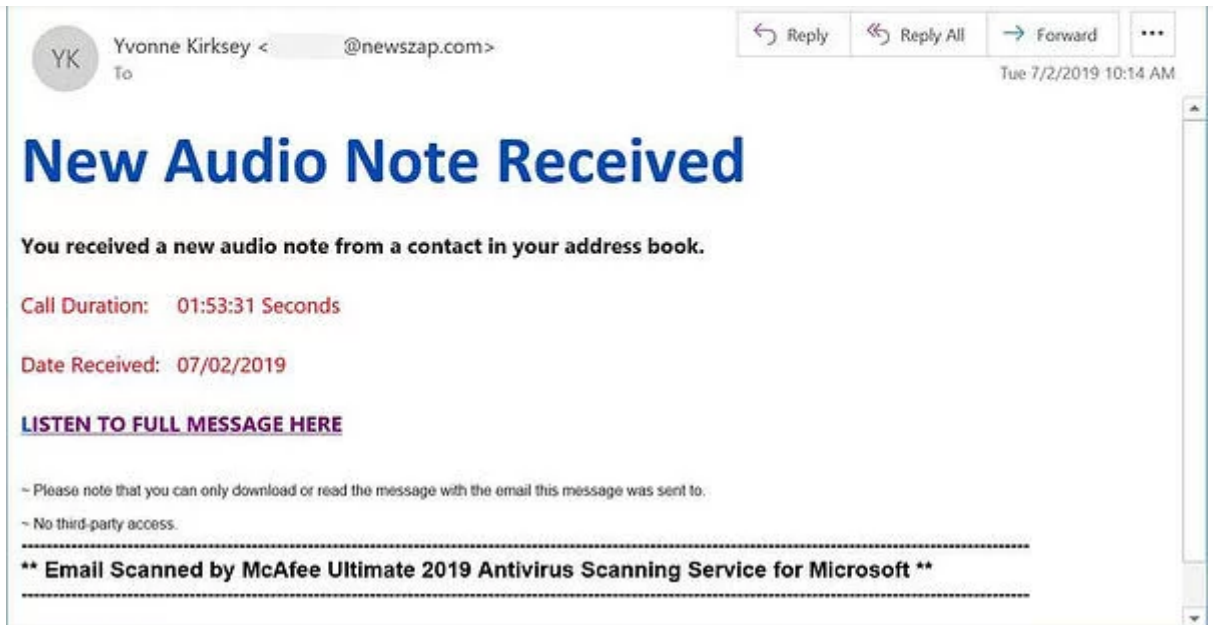
Like 54

Share

Phishing scammers are coming up with more innovative methods to convince their targets to provide login credentials. Such is the case with a new OneNote Audio Note phishing campaign that is currently underway.

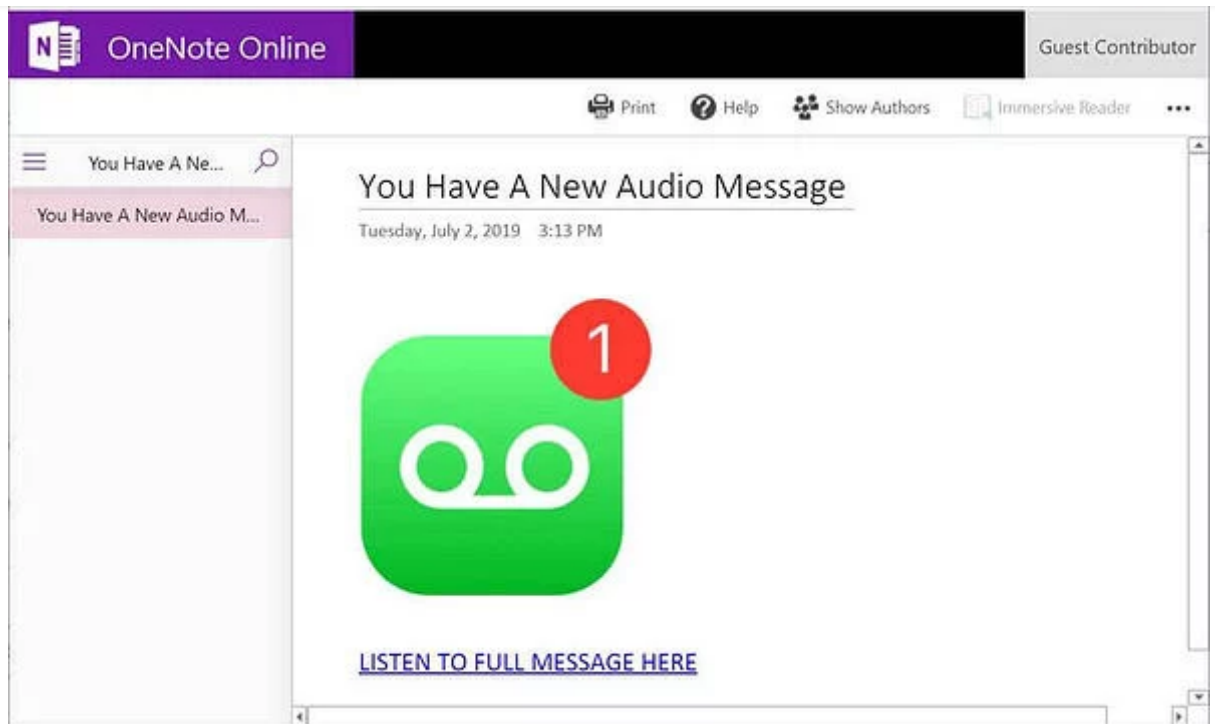
Bleepingcomputer [reported](#) that: "This campaign comes in the form of an email with the subject "New Audio Note Received" and claims that you have received a new audio message from a contact in your address book. In order to listen to the message, though, you will need to click on a link to listen to it.





Of particular interest is that the phishing scammers are now commonly including footer notes stating the email is safe as it was scanned by a security software. In this case, the email states it was "Scanned by McAfee Ultimate 2019 Antivirus Scanning Service for Microsoft".

When you click on the "Listen to full message here" link, you will be brought to a fake OneNote Online page hosted on Sharepoint.com. This page states that "You have a new audio message" and then prompts you to click on a link to listen to it.



I suggest you send the following to your employees, friends and family. Feel free to copy/paste/edit:

ALERT: Internet Criminals are sending phishing attacks where they try to trick you into listening to a fake "Audio Note". They show you screen shots and attempt to scam you into clicking on links or even log into a fake Microsoft login page.

For Microsoft accounts and Outlook.com logins, it is important to remember that Microsoft login forms will just be on microsoft.com, live.com, microsoftonline.com, and outlook.com domains *only*. If you are presented with a Microsoft login form from any other URL, avoid it and use your normal bookmarks to go to these sites.

Let's stay safe out there.

Warm regards,

Stu Sjouwerman,

Founder and CEO, KnowBe4, Inc.