September 2020 ♦ Issue 9

Solutions

INSIDE THIS ISSUE

AaSys Group will be closed on Monday, October 12, 2020 in observance of Columbus Day.

Microsoft Office 2010 End of Life

A 2017 IT Marketplace Spiceworks survey showed that 83 percent of companies are still using Microsoft Office 2010, despite the availability of newer versions such as Microsoft Office 2019 and Microsoft 365. However, on October 13, 2020, Microsoft will no longer support the 2010 version of Office. Like other software manufacturers, Microsoft is continually improving speed, security, and other capabilities to make using their products as easy and beneficial as possible. Microsoft Office 2010 EOL (end of life) means no more technical support, no more patches, and no more security updates that help protect your PC from harmful viruses, spyware, and other malicious software that can steal your personal information.

"Hackers use "Patch Tuesday" as learning opportunities so they can figure out new attacks on end of life applications."

Running EOL software can put your organization and your data at great risk. Having Microsoft applications that don't have security patches is a hackers dream. Cybercriminals review patches released for current Microsoft products and figure out what the vulnerabilities are to the current applications. Those same vulnerabilities are in the older applications and with that knowledge they are able to craft attacks that exploit those vulnerabilities. Hackers use "Patch Tuesday" as learning opportunities so they can figure out new attacks on end of life applications. In 2017, the WannaCry ransomware attack took advantage of a vulnerability in Windows XP, Windows 8 and Windows 2003, all EOL products that were no longer supported. The attack quickly self-replicated and spread to a number of other computers. That attack and the speed in which the virus was replicated prompted Microsoft to do something it had never done before and provide patches for software they deemed EOL.

It is unsure if that will be the case again on another attack of EOL products, making it even more important to upgrade to a newer version of Office before the deadline. Therefore, upgrading to Office 2019 or Microsoft 365 is imperative. In addition, updating the software will also ensure your organization will remain in compliance, meet regulation standards, and stay within your budgetary limitations.

Continued on page 2

AaSys®
Solutions are our Business

Aside from the security concerns, another benefit that will no longer be available to EOL product users is the use of phone or chat support and not being able to access updated online support content. Additionally, Outlook 2010 will no longer be able to connect to Exchange Online so users will no longer be able to send or receive emails. The caveat to this is that due to the Coronavirus pandemic, Microsoft has decided to postpone this particular change until sometime in 2021.

Although migrating to new versions of software can pose some challenges and may seem daunting, the upside is being able to have access to many new features and apps increasing ease of use and productivity, while also protecting your business from security vulnerabilities.

If you're not sure where to begin when it comes to switching from Office 2010 to Office 2019 or Microsoft 365, don't worry; AaSys is here to help! We understand the importance of keeping your organization's network running like a well-oiled machine, especially during the pandemic while remote work is now the new norm and security concerns are at an all-time high. Contact your Account Executive today so they can provide you with the best advice on how to transition to an upgraded version of Microsoft Office.

Here are some other dates to keep in mind for upcoming Microsoft EOL software:

Microsoft Product	End of Life Date
SQL 2012, SP4	July 12, 2022
Windows 8.1	January 10, 2023
Windows Server 2012 R2	January 10, 2023
Office 2013	April 11, 2023
Windows Server 2012	October 10, 2023
SQL 2014 (SP3)	July 9, 2024
Office 2016	October 14, 2025
Exchange Server 2016	October 14, 2025
Windows Server 2016	January 11, 2027

Sources:
https://www.microsoft.com/en-us/microsoft-365/office-2010-end-of-support#:~:text=End%20of%20support%2C%20which%20is,2010%20on%20October%2013%2C%202020.
https://www.pcworld.com/article/3481650/microsoft-ends-support-for-office-2010-october-13-2020-what-you-can-do.html
https://www.zdnet.com/article/microsoft-warns-office-2010-support-is-ending-so-buy-office-365-proplus/
https://www.lifewire.com/office-2010-end-of-life-4163841
https://www.spiceworks.com/marketing/resources/reports/2017-state-of-it/

Top Ten Phishing Themes of 2020

Sophos, a well-known company that creates antivirus and encryption software, has also created a product that offers users a chance to experience a realistic view of a phishing attack in order to get a better understanding of the look and feel of a real phishing scam. The Phishing Threat Simulator allows users to create their own scam templates with the hope that it will help organizations become more prepared. Sophos identified which templates were the most troubling based on click-through rates reported by users of the phishing simulator.

Here is a look at the top ten threats, not listed in order of success:

1) **Rules of Conduct** – with the emphasis on workplace diversity and reducing harassment, this email purports to provide new company guidelines.

2) **Delayed year-end tax summary** – This email allegedly advised employees as to when tax documentation would be available.

3) **Scheduled server maintenance** – With so many people working from home, people want to know when outages will occur in order to have work arounds.

4) **Task assigned to you** – This phishing campaign is somewhat different in that the Phish Threat manager is able to identify the project scheduling tool used by the organization. Although this makes the campaign a semi-targeted attack, it is not impossible to identify software and tools being used by specific companies.

5) **New email system test** – This campaign enlisted employees' assistance in testing a new system.

6) **Vacation policy update** – With COVID-19, many companies are altering their PTO policies. Employees just want to stay up to date on new requirements.

7) **Car lights on** – The message of this campaign indicated that someone had left their lights on. A link was provided, and employees were encouraged to click on the link to see a picture of the car with the lights on.

8) **Courier service failed delivery** – This tried-and-true attack has more meaning today, with many of us working from home and purchasing items online for home delivery.

Continued on page 4

9) **Secure document**- The text of the email identifies the sender to be HR, and a user is encouraged to click on text to review the secured document.

10) **Social media message** – This campaign simulated a LinkedIn notification with the message "You have unread messages from Joseph." Fear of missing out (FOMO) leads employees to click on the link…even if they don't immediately remember "Joseph."

What Sophos discovered is that although the templates covered a broad range of phishing themes, none of them were actual threats. Most of them dealt with issues that were mundane and undramatic, while at the same time apparently being interesting, important, or both.

As Paul Ducklin, the author of the report, indicates, "these results are useful in giving us a feeling for how the phishing scene is evolving. It's as though the crooks have woken up to the saying that you catch more flies with honey than with vinegar."

Key Take Away

Phishing scams are not going away; in fact they are more prevalent and sophisticated than ever before. Spam filters and antivirus do help keep many phishing emails at bay, however, nothing is foolproof. It is imperative that extra layers of precaution are always implemented.

Always Remember:

⇒ Think before you click! Don't click on links that appear in random emails and instant messages. Look for clues. Check the domain name and don't be fooled by "look alike" or "close" domain names.

⇒ Keep your browser up to date. Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers discover and try to exploit

⇒ Check with the sender if you aren't sure or aren't expecting an email from them.

⇒ Do not enter personal information in a pop-up screen.

⇒ Report suspicious emails to your IT department or security team. If you're the first in the company to spot a new scam, an early warning will let your IT department warn everyone else who might have received it too.

Sources:
Author Ducklin, Paul "Phishing tricks – the Top Ten Treacheries of 2020" Naked Security by Sophos, September 4, 2020 https://nakedsecurity.sophos.com/2020/09/04/phishing-tricks-the-top-ten-treacheries-of-2020/

https://www.phishing.org/10-ways-to-avoid-phishing-scams