Brandon Vigliarolo and Tech Republic, a leading technology publication, provide us a compelling overview of how to avoid phishing attacks. The world of cyber-criminals is attacking the simplest forms of internet usage, your email, and O365 software applications.

Avoiding Phishing Attacks

Cyber-criminals have turned to phishing. It's easy, you can hit lots of people at once, and even one response in a thousand could net you a huge return. And they are hammering on your email and Office 365 software environments.

Option 1: Rely on Microsoft's junk mail filter

Outlook's junk mail filter is reportedly able to distinguish between spam, phishing, and legitimate emails and filter them accordingly, even disabling hyperlinks and the ability to reply to a message.
While this is a great feature in both the 2013 and 2016 version of Outlook it still has its holes, just like any automated filter. The best way to make it effective is to specify junk mail criteria at the Exchange server level and push those rules out using Cached Exchange Mode or via PSTs stored server-side.

Setting junk mail filters at the server level will allow administrators to specify any specific senders, any top-level domains, or even text encoding to block. Emails blocked by the junk mail filter in this way will be sent to the Exchange server's junk mail folder and users won't even see them.

Using the junk mail filter will never be foolproof, so use this method alone at your own risk.

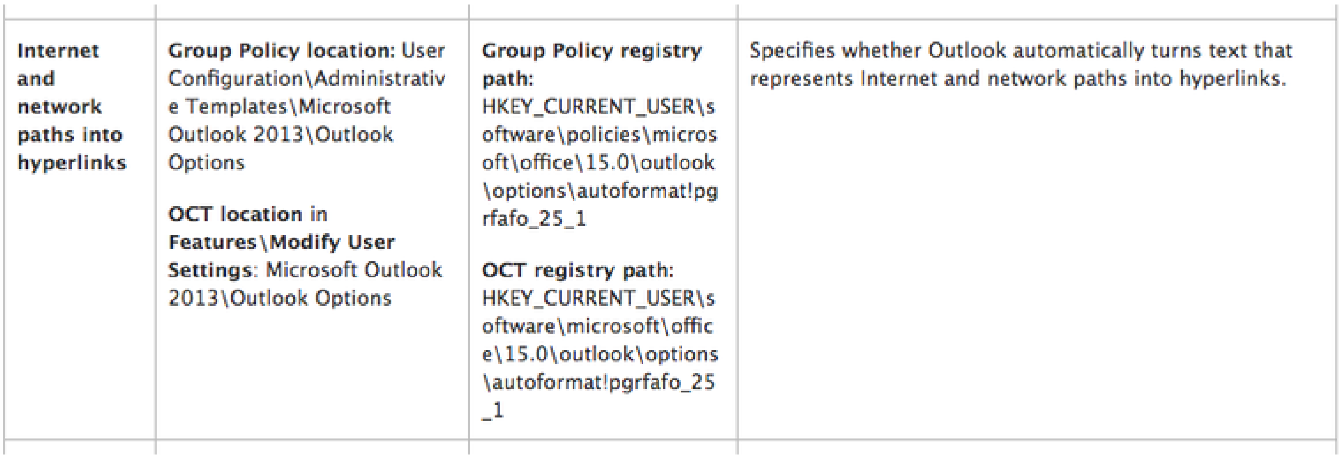
Option 2: Disable email hyperlinks using group policy

The most effective method of eliminating phishing attempts is also the most heavy-handed: Killing all email hyperlinks. By disabling any links in emails you're completely cutting off an attacker's ability to accomplish their goal: burying a false URL behind a bit of text or a legitimate looking website won't do much if it shows up in plain text.

Keep in mind this will also kill legitimate links as well—users will have to either paste full URLs into an email to be copied and pasted or simply share links in another way. Anyone doing this should be sure they get the okay from C-level decision makers: It's a huge change that may be great for security but a hassle for users.

Microsoft's website contains lots of information on how to do this for Office 2013, but not for 2016. You can download Office administrative templates for both Office 2013 and Office 2016 using similar formats and instructions but I was unable to find definitive steps for 2016.

Unless Microsoft has drastically changed the locations of Office group policy objects and registry keys, the image below, which represents the location of the object and key for Office 2013, should be similar in 2016.



Internet and network paths into hyperlinks	**Group Policy location:** User Configuration\Administrative Templates\Microsoft Outlook 2013\Outlook Options **OCT location** in **Features\Modify User Settings**: Microsoft Outlook 2013\Outlook Options	**Group Policy registry path:** HKEY_CURRENT_USER\software\policies\microsoft\office\15.0\outlook\options\autoformat!pgrfafo_25_1 **OCT registry path:** HKEY_CURRENT_USER\software\microsoft\office\15.0\outlook\options\autoformat!pgrfafo_25_1	Specifies whether Outlook automatically turns text that represents Internet and network paths into hyperlinks.

Option 3: Enable Advanced Threat Protection safe links for Office 365

Managing Office 365 is a bit different from managing a typical Office installation—and that includes enabling reliable spam and phishing filtering.

Microsoft offers what it calls Advanced Threat Protection (ATP) as an upgrade to an Office 365 subscription. One of the components of ATP is safe links, a series of filters that are applied to a message before it is sent to the recipient's inbox and after it is opened.

ATP safe links is essentially a souped-up, cloud-based version of Outlook's junk mail filter, and rules can be applied at the individual, group, or organizational level.

When applied, ATP safe links runs incoming emails (when they contain hyperlinks) through IP and envelope filters, signature-based anti-malware scans, and anti-spam filters. If found to be safe the message is sent on to the recipient.

Once opened, safe links runs a check on links in the body to see if they match organizationally blocked URLs or known bad sites. It also scans any files that are downloaded via email links.

Educate Your Users

For every weapon developed to counter spammers, hackers, and phishers, one of them comes up with a way to circumvent it. That said, it's entirely possible—if not probable—that a phishing attempt will make it past your filters someday.

Summary

The best filters and software are no match for good user education. Never miss an opportunity for teachable moments and it's not a bad idea to send out regularly scheduled security newsletters company-wide that hit on important tips and things to watch out for.

Next Steps

Connect with Oakwood. Let's get started helping you secure your most precious data and infrastructure hardware!

About Tech Republic

Tech Republic covers a myriad of technology environments and trends from the simplest to the most complex software applications. Learn more by following them at www.techrepublic.com.

Next Steps

Review our case studies and engagements where we helped companies just like yours solve a variety of business needs.

About Oakwood

Since 1981, Oakwood has been helping companies of all sizes, across all industries, solve their business problems. We bring world-class consultants to architect, design and deploy technology solutions to move your company forward.   Our proven approach guarantees better business outcomes. With flexible engagement options, your project is delivered on-time and on budget. 11,000 satisfied clients can’t be wrong.

Like what you've read? Please spread the word!