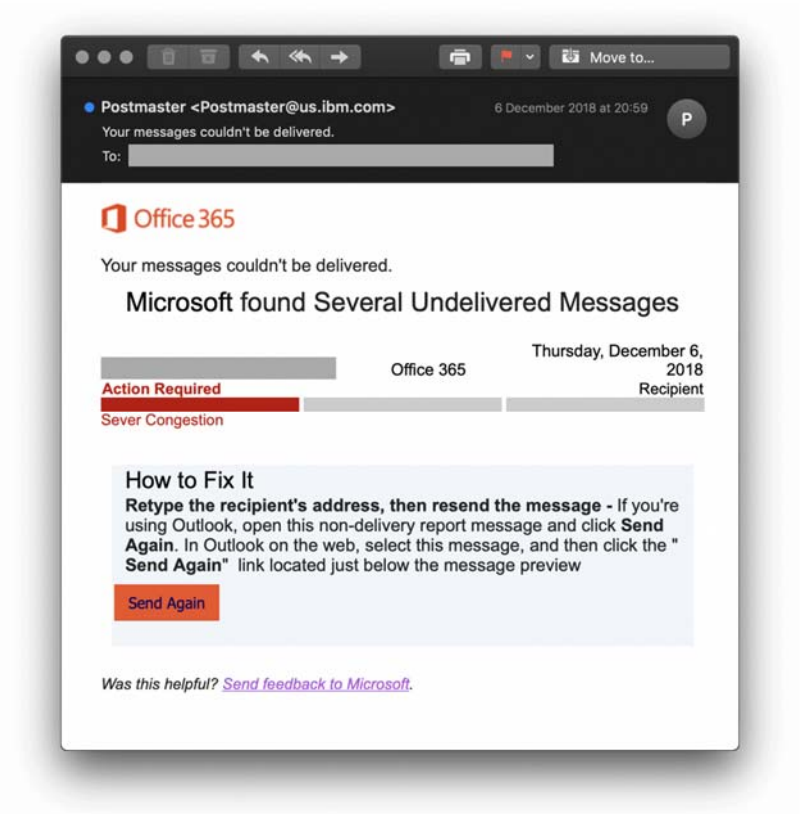
520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Office 365 Phishing Attack Using Fake Non-Delivery Notifications

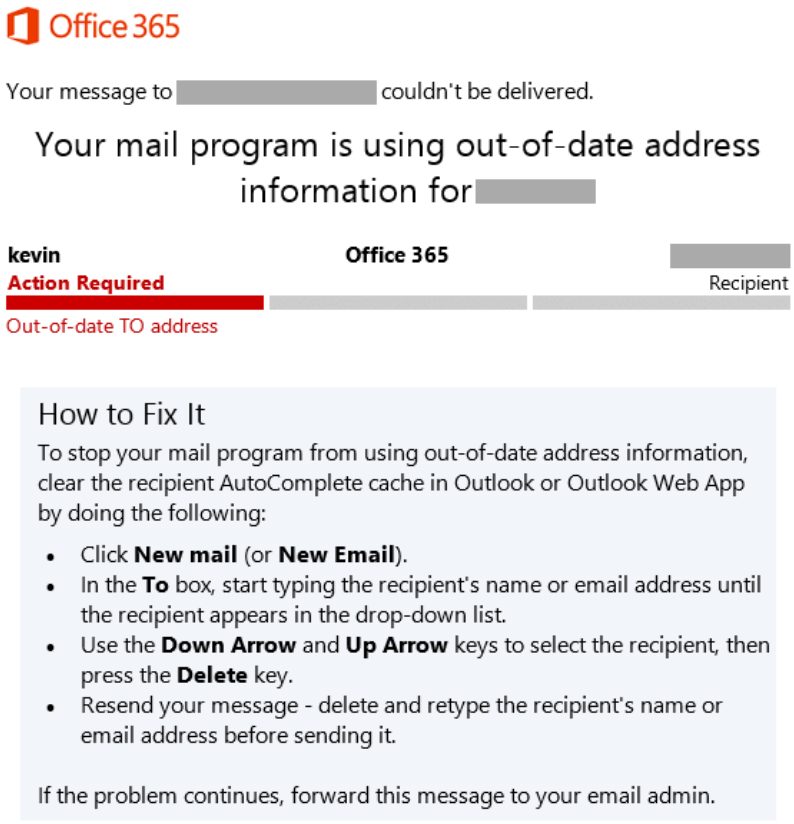
A new phishing attack is using fake non-delivery notifications in an attempt to steal users' Microsoft Office 365 credentials.

SANS ISC Handler Xavier Mertens discovered the attack while reviewing data captured by his honeypots. The attack begins when a user receives a fake non-delivery notification from Microsoft such as the one shown below:



Above is a screenshot of the fake Office 365 non-delivery notification.

For the sake of comparison, here's what a legitimate non-delivery notification for Office 365 looks like:



Office 365

Your message to [redacted] couldn't be delivered.

Your mail program is using out-of-date address information for [redacted]

kevin	Office 365	[redacted]
Action Required		Recipient
Out-of-date TO address		

How to Fix It

To stop your mail program from using out-of-date address information, clear the recipient AutoComplete cache in Outlook or Outlook Web App by doing the following:

- Click **New mail** (or **New Email**).
- In the **To** box, start typing the recipient's name or email address until the recipient appears in the drop-down list.
- Use the **Down Arrow** and **Up Arrow** keys to select the recipient, then press the **Delete** key.
- Resend your message - delete and retype the recipient's name or email address before sending it.

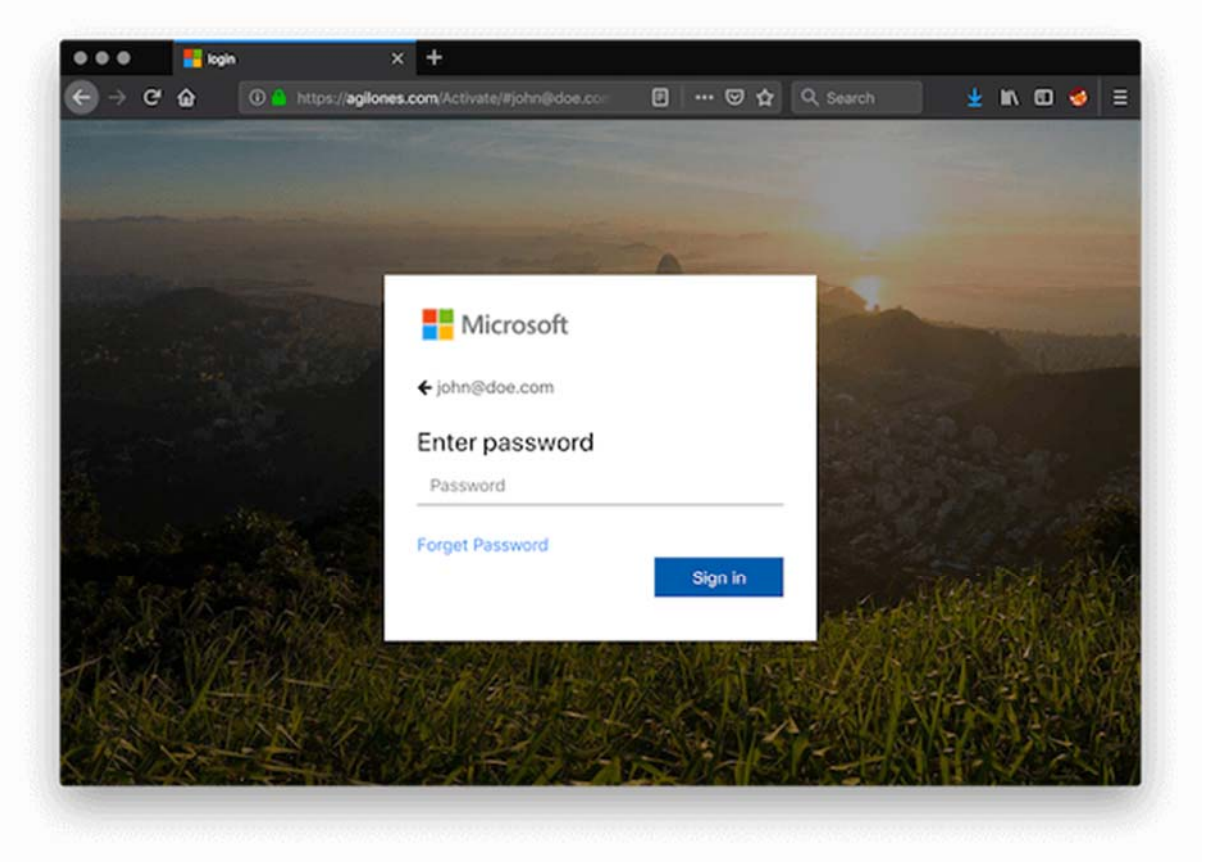
If the problem continues, forward this message to your email admin.

Was this helpful? Send feedback.

A real Office 365 non-delivery notification shown above.

As you can see, the real notification provides instructions through which the user can delete out-of-date address information for their contacts before attempting to resend the message.

By contrast, the fake notification instructs users to simply click the "Send Again" button included in the email. Doing so redirects the user to a phishing site that impersonates the real Office 365 login. The URL for the phishing page ends with *[email address] and incorporates this information into a dialog box designed to steal the user's password for their Office 365 credentials.



Screenshot of the Office 365 phishing site.

Once a user enters in their password, a JavaScript function called sendmails() sends off their information to the attackers and then redirects them to the official Office 365 login page.

This isn't the first time that phishers have preyed on Office 365 users. In 2017, bad actors used a botnet attack called "KnockKnock" to primarily target Office 365 system accounts. Just a year previously, researchers documented an attack campaign where digital attackers incorporated Punycode into fake shipping alerts to trick users into sending over their Office 365 login credentials. Always use caution when receiving emails with links in them and it is a good idea to protect your account with two-factor authentication (2FA).