Clever New Phishing Attack Is Hitting Office 365 Accounts

Phishing emails are very popular tools for cybercriminals. They send them out relentlessly, hoping that their casted nets are big enough to reel in a few victims here and there.

As usual, these opportunistic scammers craft emails and websites that look like the real deal. Recognizing these fake messages can be difficult to the untrained eye.

Take this new attack, for example. All it takes is a careless click and these criminals can take over your entire Office 365 account! Read on and see all the characteristics of this attack so you won't be the next victim.

New Office 365 phishing attack

A new phishing attack has been spotted and it is designed to steal Microsoft account credentials by sending out emails that look like email non-delivery notifications from Office 365.

Here's an image of the attack so you'll know what to look for:

The campaign was discovered by security researcher Xavier Mertens while reviewing the recent data collected by his email "honeypots." **Note:** A honeypot is a decoy computer or email account used by experts to lure and trap malware or spam attacks.

It starts with an email that pretends to be a non-delivery receipt from Office 365 saying that Microsoft found

several undelivered messages in your account.

Conveniently enough, the phishing email comes with a “Send Again” button which then pulls up a phishing page that looks exactly like the real Office 365 login tool.**Kim Komando, excerpt posted on SouthFloridaReporter.com, Dec. 18, 2018**