# 5 Steps to Protect Your Office 365 from Evasive Phishing

ISSUE BRIEF

## Defense-in-depth is essential to protect Office 365 users from sophisticated phishing attacks

Microsoft Office 365 is one of the world's leading software platforms, boasting 135 million active business users. It provides various packages that include productivity, collaboration, and communications applications, as well as capabilities to secure these apps, the platform, and users. Many organizations are adopting a defense-in-depth strategy to protect Office 365 email users from sophisticated phishing threats.

### Phishing is today's #1 cyber security threat

**Phishing is the top source of security breaches**—Growth in phishing has made it the top threat concern among IT managers with Office 365 deployed, just ahead of ransomware, according to an October 2018 survey by Osterman Research. This concern has a real basis—in the same survey, phishing was also the top reported source of security breaches, with 54% of organizations using Office 365 reporting having suffered a successful phishing attack in the prior 12 months. And usually not just one—the average number of successful phishing breaches reported per organization for the preceding year was 11.7.

**IT managers see growing phishing volumes reaching users**—Phishing has become a major problem and some security infrastructure can cope with it better than others, with both surveys and controlled email tests confirming that increasing numbers of phishing emails are evading current security and reaching business users, independent of the email platform in use. In the same survey cited above, 45% of IT managers and security administrators admins said that the number of total phishing emails reaching their Office 365 users had increased dramatically over the past 12 months, and estimated an average increase of 25%, with over half reporting a 26% increase in targeted spear-phishing. The increased success of phishing is tied to an increase in activity in the "phishing industry". Cyren's own automated monitoring of active phishing URLs globally showed a whopping increase of 172% in the eighteen months to the end of 2017, to over 10 million active phishing URLs at any given moment.

**Real-world testing shows 7.2% "miss rate"**—In real-world testing, results from email security assessments conducted by Cyren confirm the problem. Aggregated data from Email Security Gap Analysis tests across multiple companies with different security solutions, including Office 365, show a 7.2% miss rate—meaning 7.2% of all emails delivered to users were either spam, phishing or carrying malware attachments. Examining a sample of 2.7 million emails in more detail, we found that over 7,000 of these were phishing emails. As the speed and evasiveness of phishing attacks increases, detecting and updating protection quickly enough—in seconds or minutes, not hours or days—poses a major challenge for traditional email security architectures.

### What you can do to protect office 365 email users from phishing

1. **Automate email and web security threat updates to the shortest possible time interval.** You need to make sure there isn't a time lag in protection from new, emerging threats.
2. **Supplement Office 365 native email security with cloud-based email gateway protection from a security provider.** Cloud-based secure email gateways add more advanced security like time-of-click URL analysis, in-line sandboxing, and more robust protection from phishing and spear phishing.
3. **Deploy a web security gateway.** An effective web security gateway will block connections to phishing websites and botnet Command & Control servers.
4. **Use multi-factor authentication.** Password re-use makes phishing attractive for criminals. Deploy multi-factor authentication on Office 365 to prevent email account compromise.
5. **Continuously train users.** Educate users about the social engineering tricks that are used, test them, and repeat on an ongoing basis.

L8 Solutions

CYREN

**25B**
Security Transactions Daily

**1.3B**
Users Protected

**300M**
Threats Blocked Daily

**Web security is also failing**—When email security fails to block a phishing email and the user clicks on the link in it, you can still protect the user by blocking the connection to the phishing URL. Cyren offers a free Web Security Diagnostic that evaluates the effectiveness of any given user's web security in blocking phishing sites, along with other checks performed. To date, over 20,000 diagnostics have been run and 62% have failed a basic phishing URL test, while 75% have failed a separate zero-day phishing test, which checks whether a user is being allowed to access a phishing URL that is new in the last 24 hours. This is happening in part because much web security infrastructure has been architected in a manner similar to email security, and suffers the same "window of vulnerability" problem—the time between a threat being detected and protection updates being applied lags behind the speed of modern threats.

**Companies are trying user training, but lack consistency**—In the Osterman Research survey, 94% of IT managers reported that they have conducted phishing awareness training at some point for their users, showing it to be considered an accepted and integral part of a defense-in-depth strategy. However, it is accepted that even the most well trained user will often have trouble identifying a well-designed phishing email, and some percentage of users seem impervious to training. In addition, one-time training is never enough. Study after study suggests that ongoing training is required. Yet, only 19% of these same respondents engaged in regular training reinforcement.

> "With sophisticated hacking mechanisms, a perpetrator will target weakly guarded transactions and, for instance, send the buyer an email from an address nearly identical to the closing agent's, with a plausible subject line, advising of a 'wiring change'."
>
> **GOVERNMENT ADVISORY ON REAL ESTATE WIRE TRANSFER FRAUD, APRIL 10, 2018**

## Common phishing attacks and their impact

Among the types of phishing Office 365 customers need to protect against are:

**Credential phishing**—Email senders typically pose as well-known brands, social websites, or online merchants, such as Apple, Amazon, Facebook, and Microsoft. The email will contain a link that directs a user to a fake sign-in page designed to steal login information. Credential theft is a particular problem as users often use the same passwords for personal and business accounts, exposing their employer. The attacker can now try and use the phished credentials to access business applications. For example, to log in to Office 365 and gain control of the user's email, access Salesforce.com to steal customer information, or enter your financial systems.

**Financial phishing**—Email senders typically pose as a well-known financial entity and encourage the recipient to validate their business account or warn of an unauthorized transaction. If a user clicks the link they are taken to a fake website, where the attacker attempts to steal their login credentials, setting the stage to enable the criminal to steal financial information and potentially funds. The result is similar to the above, except that now, the attacker may have a direct login to a high-value asset like the business' bank account.

**Spearphishing and Business Email Compromise (BEC)**—These types of phishing emails rarely contain links and are usually highly targeted. They may purport to be from an executive and frequently target a finance team member requesting funds be transferred to a supposed business partner or asking for employee tax-related information. The attacker usually uses obfuscation techniques to make the email look like it is from the sender's real email address, but if they've hacked the sender's email account, they can obviously send a "real" email. The result of BEC attacks is usually direct financial loss, even when processes are in place to prevent this type of fraud. The email recipient may disregard such processes because the attacker has managed to create a sense of urgency.