

PhishPrevent Overview

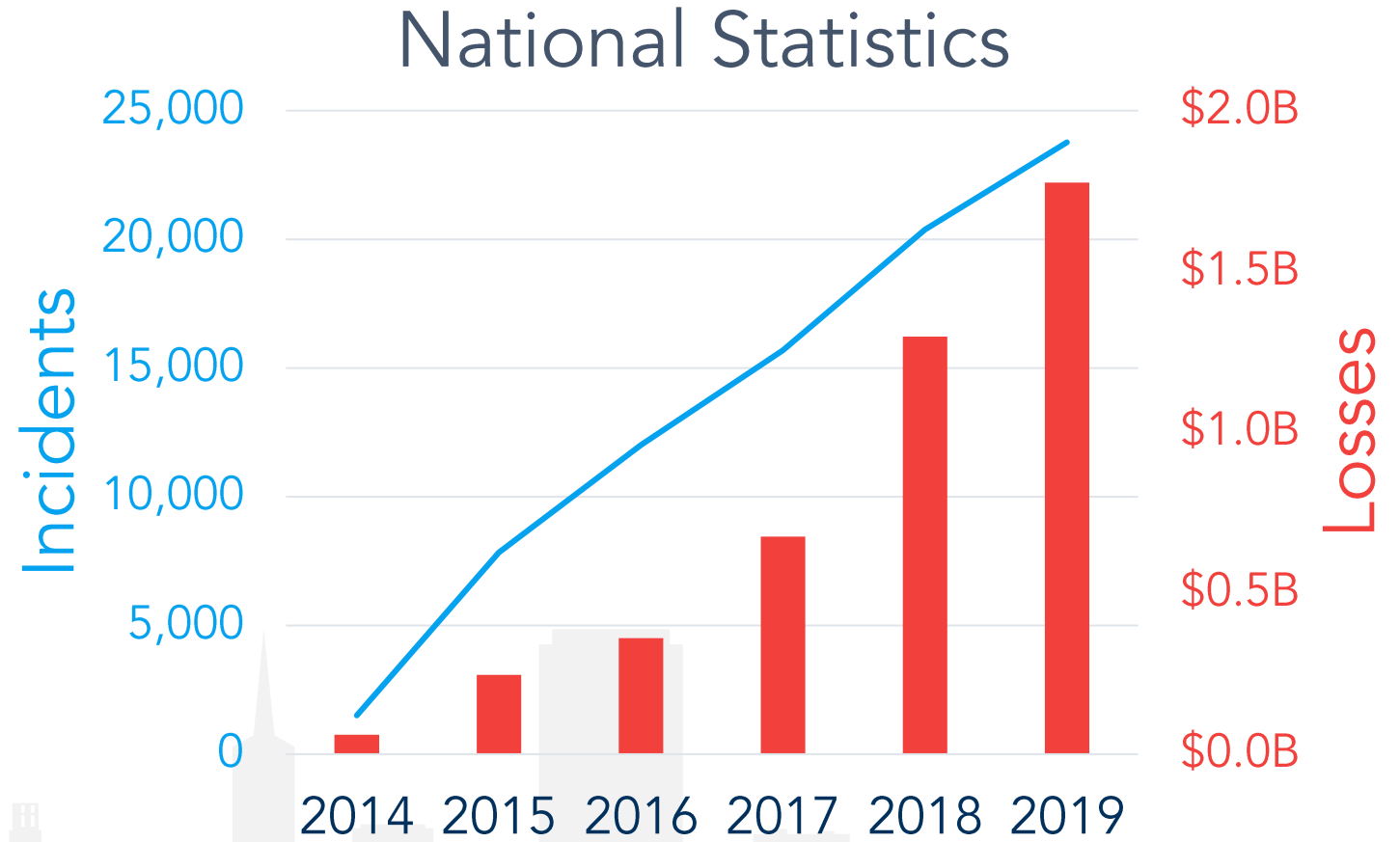
Why did we build this?

Why did we build this?

- Finchloom has been focused on implementing and managing Office 365 since our inception in 2013
- Starting in 2016, we began to see our clients suffer major financial losses to Business E-mail Compromise (BEC) attacks
- Attackers would steal credentials via phishing and then use e-mail access to trick users into wiring money, changing account numbers, etc.
- We have seen up to 4 million dollars lost in a single attack

Why did we build this?

Since then, BEC has quickly eclipsed ransomware to become the largest cybersecurity threat for all businesses



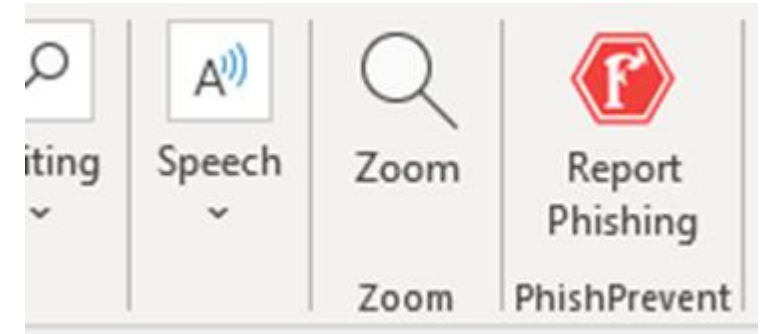
Why did we build this?

- In the process of responding to these incidents we gained a deep understanding of the techniques and tactics used by attackers.
- We set out to share and implement the mitigation strategies we collected **before** our clients get breached instead of after.
- We built PhishPrevent to take a threat-based approach to the problem and combine all the most effective mitigation strategies in one **turn-key fully managed service**.

What's included in the service?

Incident Response for Suspicious E-mails

- A large amount of malicious e-mails are getting past signature-based spam filtering and will continue to do so.
- Your users will have a new button in Outlook/OWA they can use to report suspicious e-mails to us.
- We perform a human review of all submissions and communicate with the reporter to let them know our findings and answer any questions.
- If the e-mail is malicious, we delete all other past and future occurrences of the same e-mail from other mailboxes.



User Training and Awareness

- We perform an initial webinar to educate your users about phishing, teach them what to look for, and show them how to report suspicious e-mails to us via the button.
- We perform regular phishing simulations to reinforce positive behavior.
- If a user fails a simulation by clicking the link or entering their credentials, they are directed to on-the-spot video training to show them what they did wrong and how to spot suspicious e-mails in the future.

Impersonation Warning Banners

- Users are warned when something is out-of-the-ordinary about an e-mail they received.
- Targeted messages are more effective than blanket warnings that people become accustomed to ignoring.

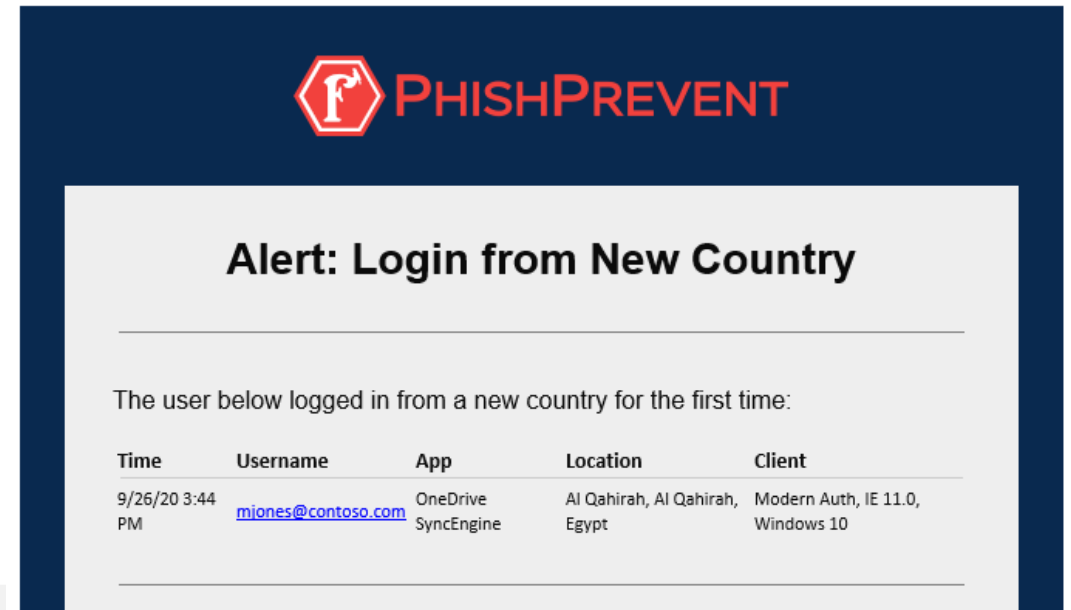
PhishPrevent Warning: this is the first time you received an email from this sender YourCEO@aol.com

PhishPrevent finds this email suspicious! We know John Smith by name, but the email was sent from an unfamiliar address jsmith@yahoo.com.

PhishPrevent finds this email suspicious! It seems like this email was sent from PayPal but it might be an impersonation attempt as it was sent from mike@amysflowershop.com.

Sign-in Activity Monitoring

- We found native Office 365 authentication monitoring features to be lacking. They generate many false positives, causing alert fatigue, and can't be customized. So we built our own!
- We fine tune alerts to minimize false positives while ensuring that highly suspicious activities are properly investigated.
- Sign-in events are correlated with receipt of known phishing e-mails for enhanced detection



The screenshot shows a PhishPrevent alert interface. At the top is the PhishPrevent logo. Below it is the alert title "Alert: Login from New Country". A message states: "The user below logged in from a new country for the first time:". Below this is a table with the following data:

Time	Username	App	Location	Client
9/26/20 3:44 PM	mjones@contoso.com	OneDrive SyncEngine	Al Qahirah, Al Qahirah, Egypt	Modern Auth, IE 11.0, Windows 10

Suspicious Domain Monitoring

- In almost all serious attacks we've seen, attackers have used e-mail domains that appear visually similar to the company's actual domains.
- We monitor for new domain registrations that look similar to your domains to get an early warning of a potential attack in progress.
- If a malicious domain is registered, we ensure your users haven't communicated with that domain and we have it taken down if needed.

As your Office 365 Security Partner

- We partner with you to ensure your Office 365 environment is always configured in a secure manner, with all current best practices implemented.
- We provide guidance and assistance with implementing and configuring Multi-Factor Authentication (MFA), Conditional Access Policies, and several other key security settings.
- As new attacker techniques and best practices emerge, we ensure you are abreast of the changes and your environment is always properly secured.

Next Step: Free Office 365 Breach Assessment

- We automatically analyze 6 areas of your Office 365 environment for Indicators of Compromise (IOCs) based on our years of collecting evidence from actual breaches.
- You will receive a report listing anything suspicious that we found for your review.



The image shows a sample of a Breach Assessment Report from PHISHPREVENT for Contoso Industries. The report is titled 'Breach Assessment Report' and 'Contoso Industries'. It includes a section for 'Logins From Foreign Countries' with a table of user logins from Croatia, Switzerland, and Taiwan. Below this is a section for 'Suspicious E-mail Protocols'.

PHISHPREVENT

Breach Assessment Report

Contoso Industries

Logins From Foreign Countries

One of the most obvious signs of a breach is if a user has logged in from a country that they haven't been to. Please review this list of users that have successfully logged in from outside North America in the last 30 days and see if any aren't expected.

Username	Country	Last Login	Login Count
cdavis@contoso.com	Croatia	8/28/2020 6:57:51 AM	42
cmendenhall@contoso.com	Switzerland	9/17/2020 12:06:20 PM	179
dlyles@contoso.com	Taiwan	9/22/2020 9:50:24 AM	18

Suspicious E-mail Protocols

When attackers compromise user credentials they often attempt to access the

Q&A