Microsoft inSITe BUSINESS SOLUTIONS

Simulated Phishing Attacks

Test Your User Susceptibility

Email Phishing Attacks on Your Organization

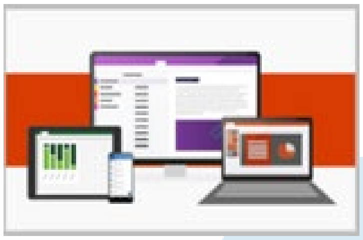
Whether your infrastructure is in the Microsoft cloud, on-premises, or in a hybrid configuration, your users, your network, and your organization's data are all susceptible to socially engineered cyber attacks.

Cyber attack vectors are changing ever day. As cloud environments become hardened against identity attacks, the vector has now shifted to the user. Most user targeted attacks are now trying to steal logon credentials.

Once able to logon as a user, attackers can then spoof emails as other internal users making them look as real as possible. When receiving an internal email, users let their guard down and are more willing to click on embedded links. The problem is that these links lead to websites that look very real, such as the Microsoft Office 365 logon page. When a user enters credentials in this site to logon, the attacker now has access to your environment.

Social Cyber Attack Simulation

- ✓ **Test** your user handling of phishing emails
- ✓ **Learn** about the latest attack vectors
- ✓ **Spear Phishing Attack** using a trusted display name
- ✓ **Password Spray Attack** using common passwords
- ✓ **Brute Force Attack** randomizing passwords
- ✓ **Educate** users who fall victim to the simulation
- ✓ **Periodic** simulations for users to remain skeptical



Targeted Phishing Email Simulations

User training about how to recognize unsolicited email and how to recognize spoofed websites is provided in many organizations, but rarely on a periodic basis. Even with the proper training, anyone can be fooled. The training must be periodically performed and reinforced through simulated activities – to see just how susceptible your users are to this threat. It is through these periodic simulations that you will remind users to be skeptical of any email they receive.

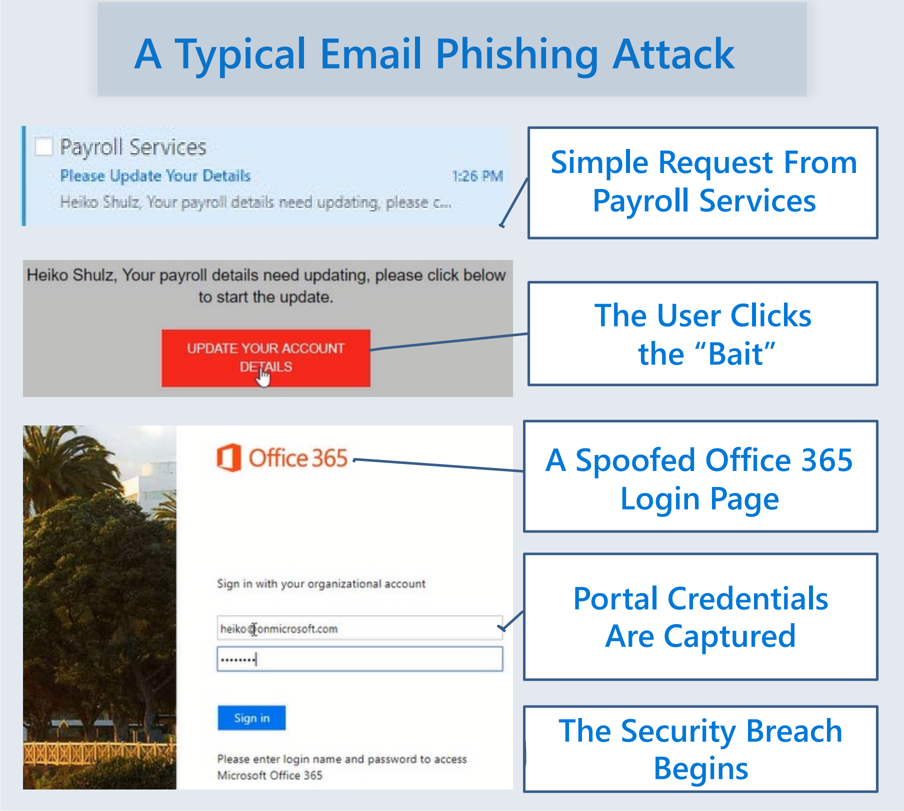
Train Your Users with Real Simulations – Train them to Question Email Validity

Organizations focus their security solutions on protection, detection, and remediation. The challenge for many organizations is how to effectively implement these solutions and test their effectiveness. No matter your organization's size, no matter the training you invest in and no matter your security posture it just takes one user to click on a malicious spear phishing link to begin a security breach of your network. Only with periodic phishing simulations can they be trained to remain vigilant by questioning the validity of every email they receive. A consistent proactive threat prevention and awareness campaign is making a measurable difference in every organization.

Microsoft insITe BUSINESS SOLUTIONS

Simulated Phishing Attacks

Enhance User Vigilance



A Typical Email Phishing Attack

Payroll Services
Please Update Your Details 1:26 PM
Heiko Shulz, Your payroll details need updating, please c...

Simple Request From Payroll Services

Heiko Shulz, Your payroll details need updating, please click below to start the update.

The User Clicks the "Bait"

A Spoofed Office 365 Login Page

Sign in with your organizational account

heiko@onmicrosoft.com
••••••••

Please enter login name and password to access Microsoft Office 365

Portal Credentials Are Captured

The Security Breach Begins

Our Enhanced Phishing Simulation

Sure there are many phishing simulators on the market to subscribe to, but none are quite like the one we use.

The Attack Simulator for Office 365 uses the Microsoft Intelligent Security Graph that is constantly learning from signals received from around the world - one of the largest telemetry systems on the planet. As an example, Microsoft Office 365 scans 400 billion emails every month, where there are a large number of malicious spear phishing emails. The Attack Simulator we use carefully crafts simulate spear phishing emails based on this real data, ensuring the most realistic attack experience on your user population.

The simulated attack tracks and reports on the user response to these emails, providing invaluable data on how to better secure the organization.

Let Us Simulate These Attacks in Your Network

We have the skilled personnel and the tools required to design, launch, and analyze the success rate of a simulated social engineering phishing attack. We go above other providers by using real display names in our simulations instead of external email addresses that are easily recognized. We are offering a one week simulated phishing attack to customers at a discounted rate. We will provide the results of simulation and suggestions to further train users and best practices to secure your environment even if and when a user is tricked in the future.

InsITe is Your Trusted Technology Advisor

We have been in business for over 20 years and have engaged with thousands of customers on a variety of products. Our company has a long standing and difficult to achieve Microsoft Gold Partner accreditation in Cloud Platform, Cloud Productivity, Collaboration and Content, Enterprise Mobility Management, Communications, and Messaging. Our business has always been focused on Microsoft technologies and was one of the first to join Microsoft in their journey to offer cloud services. Few companies can compare to our achievements and the quality of people and work products we offer our customers.

tellmemore@trustedinsite.com www.trustedinsite.com insITe BUSINESS SOLUTIONS