Stickley on Security

Domain Assure

Spear Phishing and Typosquatting Defense

Your domain is an essential part of your brand. Protect your brand by preventing cybercriminals from using your domain against you and your customers. By protecting your domain, Domain Assure can greatly curtail spear phishing and typo squatting attacks.

Spear Phishing

People who receive an email with a domain that looks almost identical to your domain are far more likely to believe the email is legitimate and trust the link or attachment. According to the *2019 Verizon Data Breach Investigation Report*, 92% of all malware infections begin with a phishing email. Locking down all the domains similar to yours is the best way to prevent them from ever being used for nefarious reasons.

Typosquatting

For as long as companies have been registering domain names, cybercriminals and competitors have been using this tactic to commit a wide range of scams. The two most common scams are tricking a user into downloading malware and to stealing a user's credential when they believe they're logging into your site.

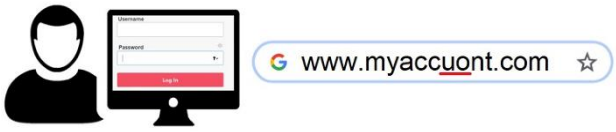
What Is Typosquatting

Also called Domain Jacking - is a cyberscam that relies on people mistyping a URL to land on a malicious website

Revenue Models

- Infect users with **malware**
- Mimic website to trick users into giving up their **login credentials and MFA**
- Redirect traffic to a **competitor**
- Generate ad clicks

Credential Theft



1. User mistypes account URL
2. Lands on malicious website that mimics trusted website
3. Enters credentials, malicious site passes credentials to trusted site and responds to User with MFA questions
4. User answers questions; malicious site passes information to trusted site and has full access to Users account
5. User is then passed off to the trusted site where they will have to login again, most Users believe it was just a glitch and do not report the incident

Malware Infection

MISTYPES URL
It's a simple mistake made by people every day

LANDS ON MALICIOUS SITE
Cybercriminals continually purchase domains that are only a typo away from the trusted website

SCAM
User is prompted to install a "needed" update

MALWARE INFECTION
Once the malware has been installed, the User is forwarded to the trusted website without suspicion

Why Domain Assure?

Monitoring domains will only alert you that a domain similar to yours has been purchased, possibly for malicious intent. Owning the domains prevents them from ever being available. SoS has a proprietary algorithm that identifies a wide variety of typo and look-alike domains, purchases them in seconds, and ensures that if a user mistypes one of these domains, they still end up at your website. Management of one or many domains is simple.

Features:

- Secure look-like and typo domains & forward them to desired domain
- Monitor and provide security reports for potential threats
- Scan for hyphenated domains (yourdomain-alert.com)
- Continually attempt to secure monitored domains owned by other organization
- Multiple domains can be protected with a single service fee

wwwStickleyOnSecurity.com
800.640.6746

The Products

No amount of infrastructure can protect an organization from uninformed employees, customers and vendors. The entire SoS product suite is focused on addressing these issues for organizations of any size or technological sophistication:

Employee EDU™. This complete cybersecurity training system is at the heart of the SoS offering. Unlike other services that update content annually, SoS believes that best practices demand quarterly updates, and furthermore that its customers should require employees to take each new course as it's issued. Our flagship product, Employee EDU is designed to meet the needs of customers that require a highly customized environment and want to take their cybersecurity training to the next level.

BadPhish™. The most notorious data breaches of all time started with an employee clicking a link in a scam email. Again, as a matter of best practices, SoS issues a new phishing email each month and expects its customer to take advantage of that. What's more, Bad- Phish can automatically assign an appropriate Employee EDU class to any employee who fails the test.

Powered Cybersecurity Training™. While suitable for organizations of all sizes, PCT was created to help solve the challenges small and medium-sized business face when deploying and managing security education and phishing simulation. It bundles the most critical features of Employee EDU and BadPhish into a fully automated solution that can be easily deployed in any environment. Once users are set up, deployment takes just a few more mouse clicks. Even reports and notices are completely automated. Although technical sup- port is always available, PCT is designed to be a self-service suite. PCT makes buying and implementing best-in-breed cybersecurity awareness, education, and training as easy as buying anti-virus software.

SoS Advisor™. As a valuable service for customers, SoS Advisor is an online cybersecurity resource center than any organization can have up and running on its website in a matter of minutes. It's based on the idea that well-educated customers translate to decreased risk for vendors. SoS Advisor also offers an optional e-newsletter to which users can subscribe. This weekly newsletter recaps the SoS Advisor articles from the previous week.

Market Differentiators

- "Canned" online training courses are known for being boring and repetitive. SoS believes that training and content must be fresh and engaging to be effective. We offer a completely new, comprehensive security course created each quarter to keep employees informed and prepared. Cybercrime is continually evolving; it's imperative that an organization's cybersecurity education keeps up. This focus on quality is just another example of our commitment to industry best practices.
- Course assignment to a failed phishing test is completely automated. Classes are short and engaging, but still deliver pertinent information to help the employee better understand the mistake and how to improve their behavior.
- Powered Cybersecurity Training provides a cost-effective, fully automated solution, putting advanced cybersecurity education and phishing simulation within reach of organizations of any size or technical sophistication. PCT is the easiest to implement and use solution on the market today, yet still brings your customers powerful results.