Blue Team Level 1 Certification (Standard)
Security Controls
5 Topics | 1 Quiz
Networking 101
6 Topics | 1 Quiz
Management Principles
4 Topics | 1 Quiz
PHISHING ANALYSIS DOMAIN
PA1) Introduction to Emails and Phishing
7 Topics | 1 Quiz
PA2) Types of Phishing Emails
10 Topics | 2 Quizzes
PA3) Tactics and Techniques Used
12 Topics | 2 Quizzes
Section Introduction, Tactics and Techniques
Spear Phishing
Impersonation
Typosquatting and Homographs
Sender Spoofing
HTML Styling
Attachments
Hyperlinks
URL Shortening Services
Use of Legitimate Services
Business Email Compromise
[Video] Tactics and Techniques & Examples
Activity) Reporting on Tactics Used
Activity) End of Section Review, Tactics and Techniques
PA4) Investigating a Phishing Email
8 Topics | 2 Quizzes
PA5) Analysing URLs, Attachments, and Artifacts
8 Topics | 1 Quiz
PA6) Taking Defensive Actions
12 Topics | 1 Quiz
PA7) Report Writing
7 Topics | 1 Quiz
PA8) Phishing Response Challenge
3 Topics | 1 Quiz
THREAT INTELLIGENCE DOMAIN
TI1) Introduction to Threat Intelligence
7 Topics
TI2) Threat Actors & APTs
6 Topics | 2 Quizzes
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz
TI5) Strategic Threat Intelligence

# Typosquatting and Homographs




This lesson will cover two visual-based tactics used to trick recipients into thinking that an email address or domain is legitimate; typo squatting and homographs.

## TYPOSQUATTING

Typo squatting is the act of impersonating a brand or domain name by misspelling it, such as missing letters or including additional ones. Below are some examples of domains that are typo squatting the real SBT domain, securityblue.team.

- **securltyblue.team**
- **securitybllue.team**
- **securtyblue.team**

At a glance, they all look somewhat legitimate. It's only when you really focus on them that you can identify the issues.

- **The 'l' in "security" is actually a lowercase L**
- **There are two L's in "blue"**
- **There is no 'l' in "security"**

Large organizations may choose to generate a list of similarly-named domains, and either use a monitoring solution to see if someone has registered any of them, or they can pay the cost to register them under the business name, preventing anyone else from taking them.

**We've purchased one of our potential typo squat domains, securltyblue.team – check it out!**

## Typo squatting Example Walkthrough

This tactic is used when registering a domain, as it allows the typo squatted name to be used for a website, and even custom emails. Let's walk through a mock scenario, where attackers want to send a spear phishing email to a member of the HR department at Dickson United, in order to retrieve personal information on an employee working in the company's IT service desk as preparation for blackmailing the employee into providing the hackers with remote access to company servers.

The hackers know that John Doe is a service desk analyst within the IT support team at Dickson United. Samantha Moore is new to the organization, and works in HR. The domain for the organization is DicksonUnited.co.uk – so the attackers decide to register DicksonUnted.co.uk.

DicksonUnited.co.uk
DicksonUnted.co.uk

The attackers discover Samantha's work email address based on a standard naming convention (samantha.moore@DicksonUnited.co.uk). Because the attackers own the typo squatting domain, their web host also offers webmail accounts through Office365, meaning the attacks can create an email address such as "anything@dicksonunted.co.uk". The attackers decide to pose as a senior HR manager Chloe Wood. They register the mailbox "Chloe.wood@dicksonunted.co.uk".

They send the tailored email to Samantha Moore, posing as the senior HR manager Chloe Wood. At a glance, the typo squatting sending email address looks completely legitimate. Samantha believes she is being contacted by her

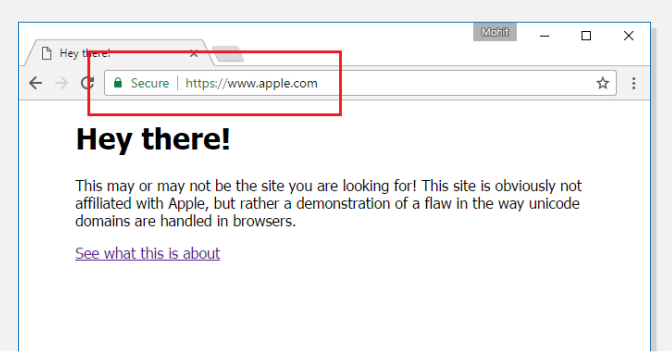
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz

superior and completes the request, sending "Chloe" personal information on the true target, John Doe.

# HOMOGRAPHS

A homograph phishing attack is virtually impossible for users to spot. This attack exploits the fact that many different characters look exactly alike. These characters are called homographs, and the problem is with how the characters are encoded using Unicode.

Wikipedia summarizes that "Unicode incorporates numerous writing systems, and, for a number of reasons, similar-looking characters such as Greek O, Latin O, and Cyrillic O were not assigned the same code. So, the Latin "o" and the Cyrillic "o" have a different Unicode and are therefore different letters." It also means domains with those two different Os are two different domains. Domains using non-Latin letters are referred to as internationalized domain names (IDN) and are used quite frequently in homograph attacks.




The scary fact is that users can't spot this attack, meaning that security awareness training is ineffective at preventing users from interacting with phishing emails that utilise homographs for domain names and email addresses. This issue needs to be addressed using effective email security technology, such as tools that visit hyperlinks within emails to identify if they are malicious or not.

A great example of a homograph attack is the article by BitDefender titled "New Homograph Phishing Attack Impersonates Bank of Valletta". Another good resource is this article by The Hacker News that talks about homograph attacks.

Previous Topic
Back to Lesson
Next Topic

Privacy & Cookies Policy