ARIZONA SMALL BUSINESS BOOT CAMP & COLLECTIVE

RESPOND → PLAN → RETURN STRONGER

CYBER SECURITY TRAINING AND CONSULTING LLC

Holiday Hacking

PRESENTED BY

Jeffrey Crump & Chris Alexakis

Copyright

Learning objectives

1. The most common threats facing SMBs
2. Securing your site using certificates
3. Email protection steps (SPF, DKIM, DMARC & BIMI)
4. Simple resilience to ransomware

The most common threats facing SMBs

How small- and medium-sized business are targeted

Spoofing

- Website
- People

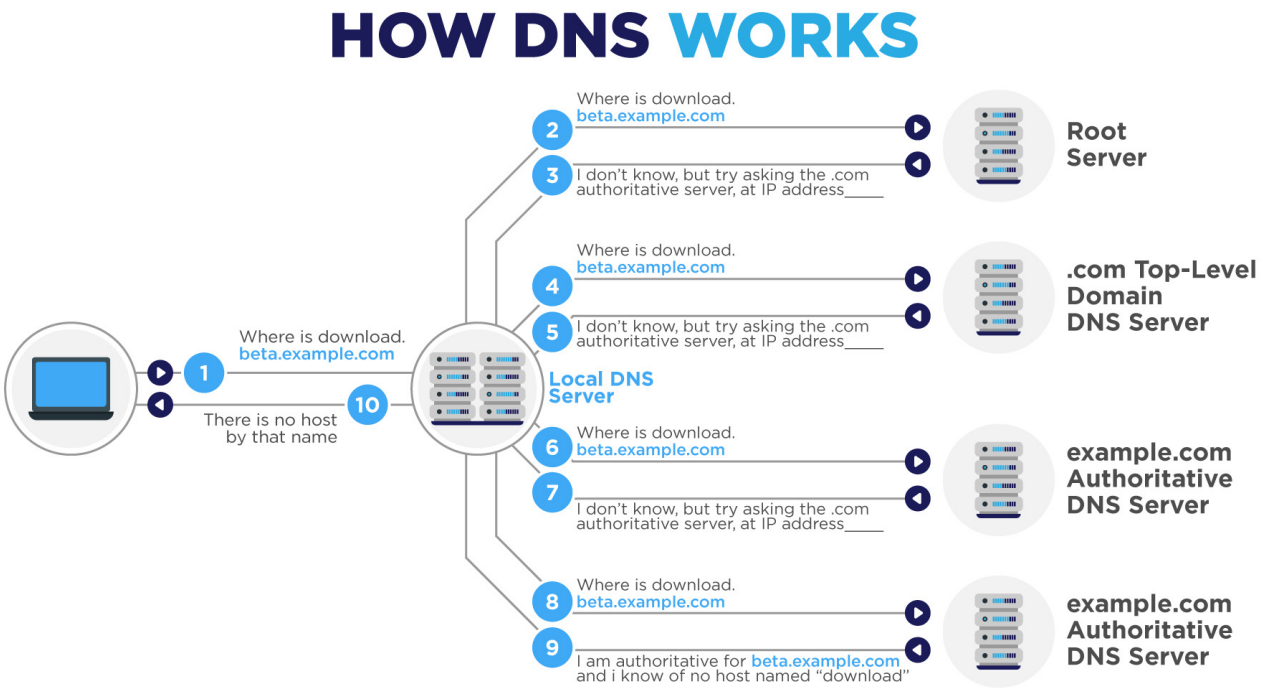
Phishing

- Phishing
- Spearphishing
- Vishing
- SMiShing

Ransomware

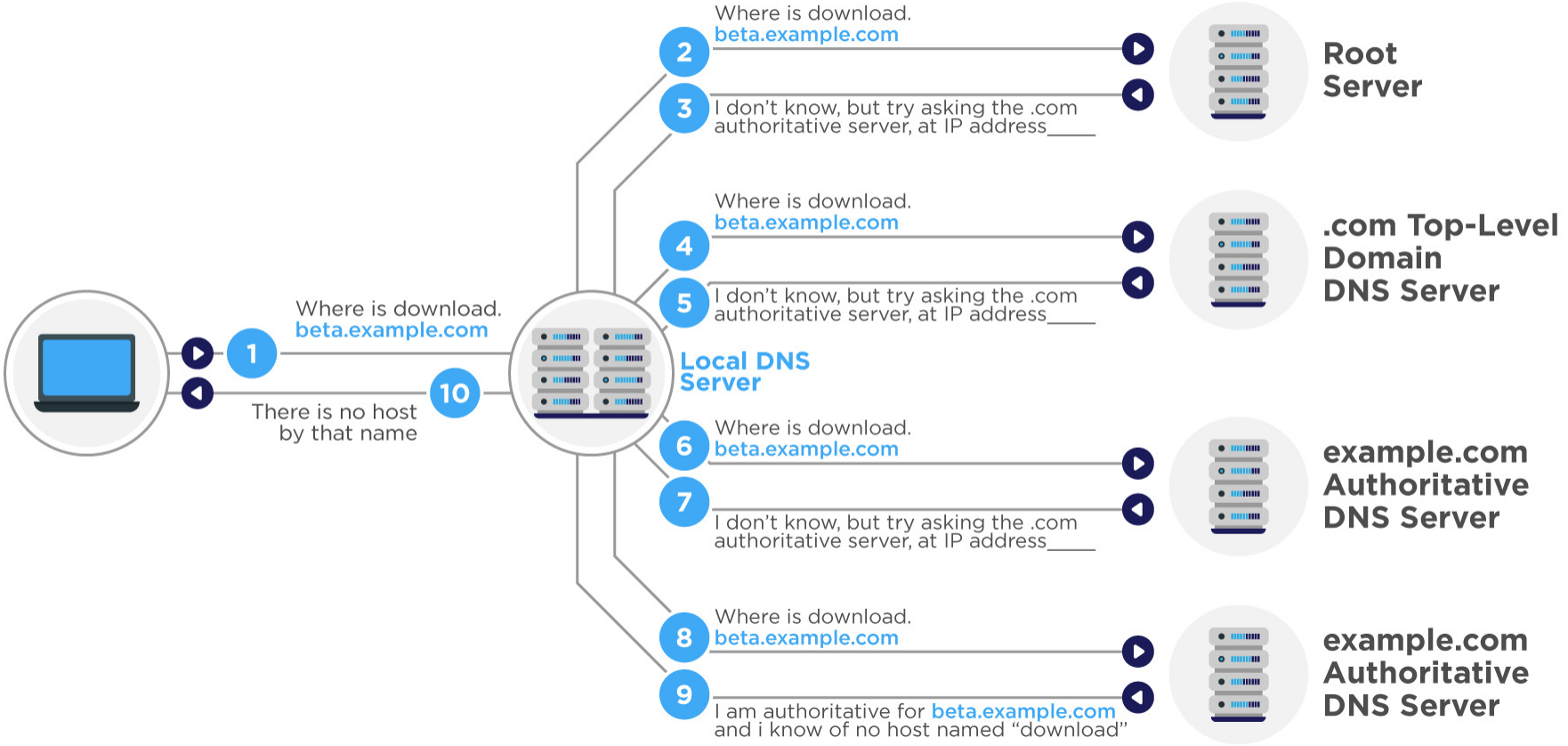
- Building resilience

Spoofing: Website



DNS: What is a Domain Name Server and why does it matter?

HOW DNS WORKS



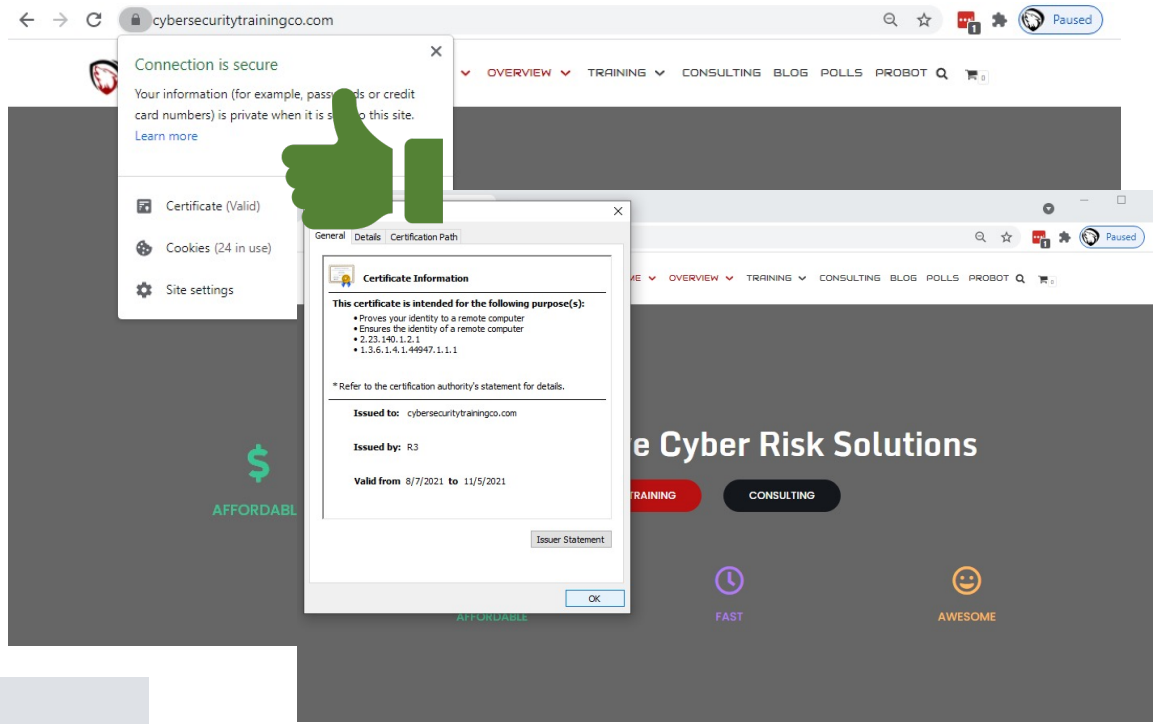
Spoofing: Website

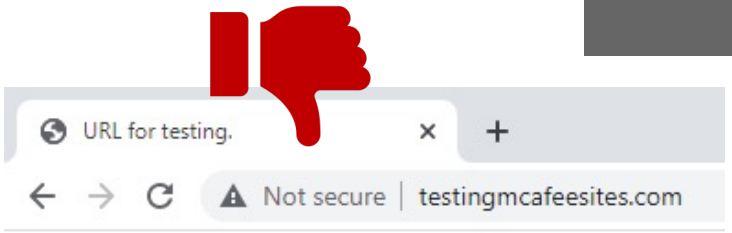
Site Certificates

- Purpose
- Certificate Authorities (CAs)

Live Demonstration: Installing a website certificate

- GoDaddy
- Siteground



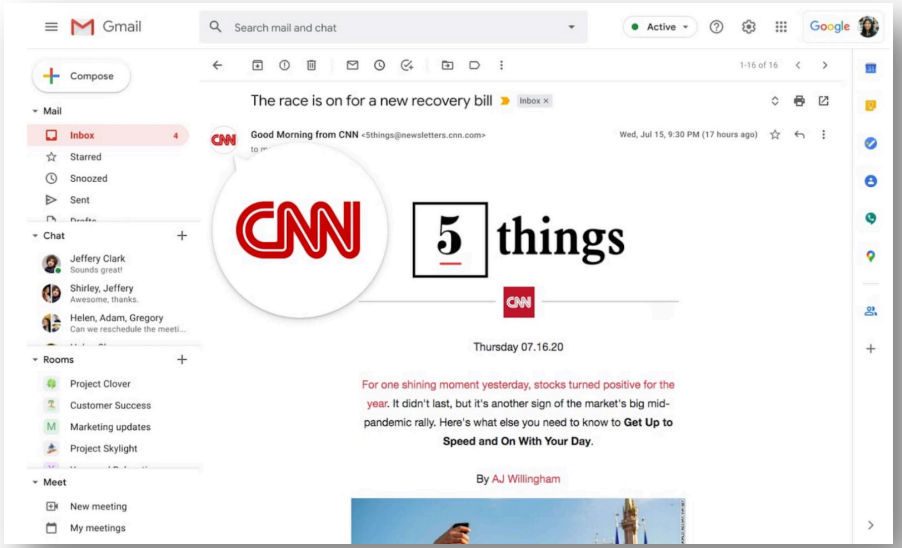


LIVE DEMONSTRATION

Spoofing: People

Anti-Spoofing Tactics

- **SPF**: Sender Policy Framework (SPF) detects forged sender addresses during the delivery of the email.
- **DMARC**: Domain-based Message Authentication, Reporting and Conformance is an email authentication protocol.
- **DKIM**: DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in email (email spoofing).
- **BIMI**: Brand Indicators for Message Identification, or BIMI (pronounced: Bih-mee) is a specification allowing for the display of brand logos next to authenticated e-mails.

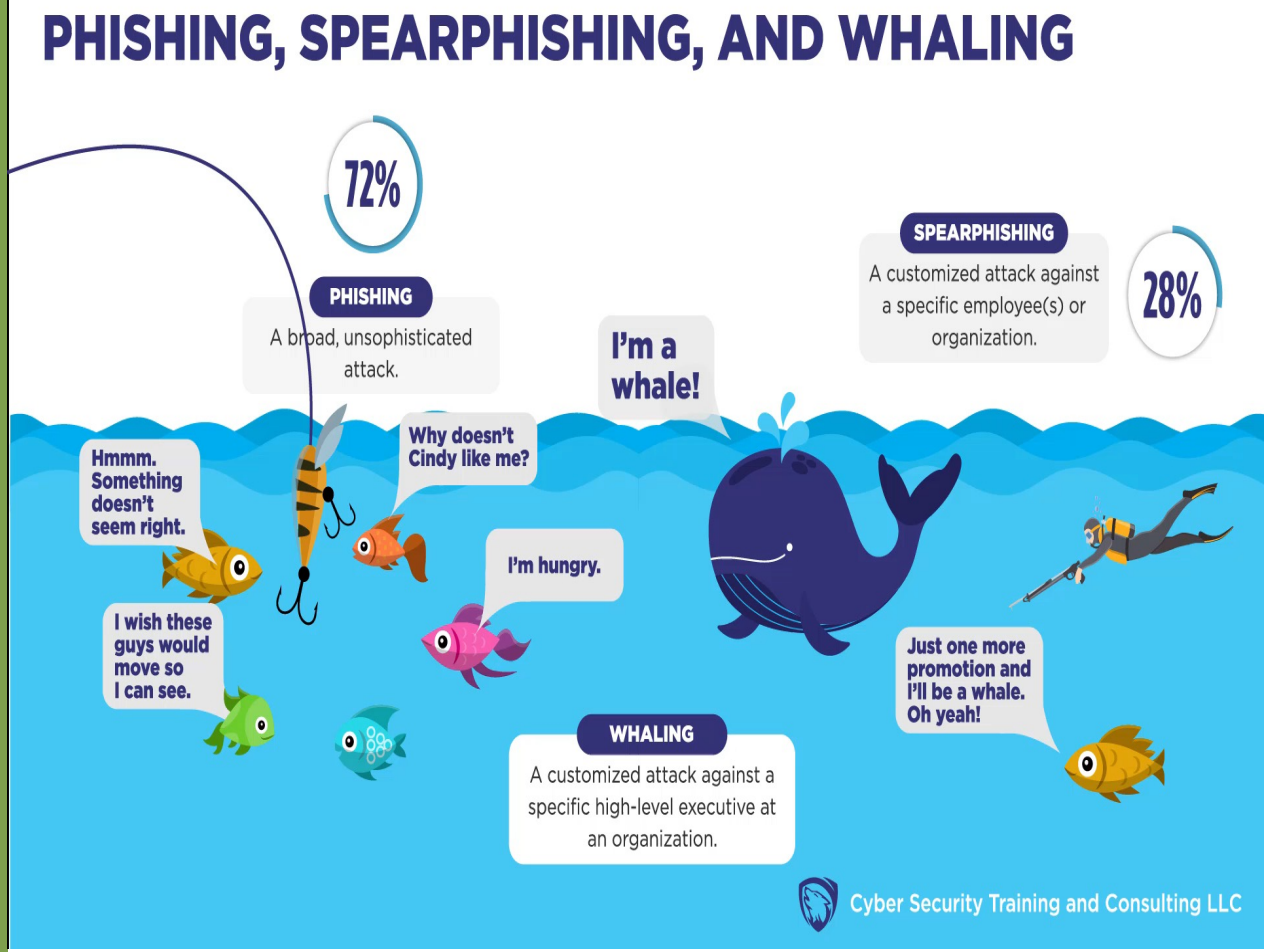


Live Demonstration: Configuring SPF, DMARC, and DKIM

LIVE DEMONSTRATION

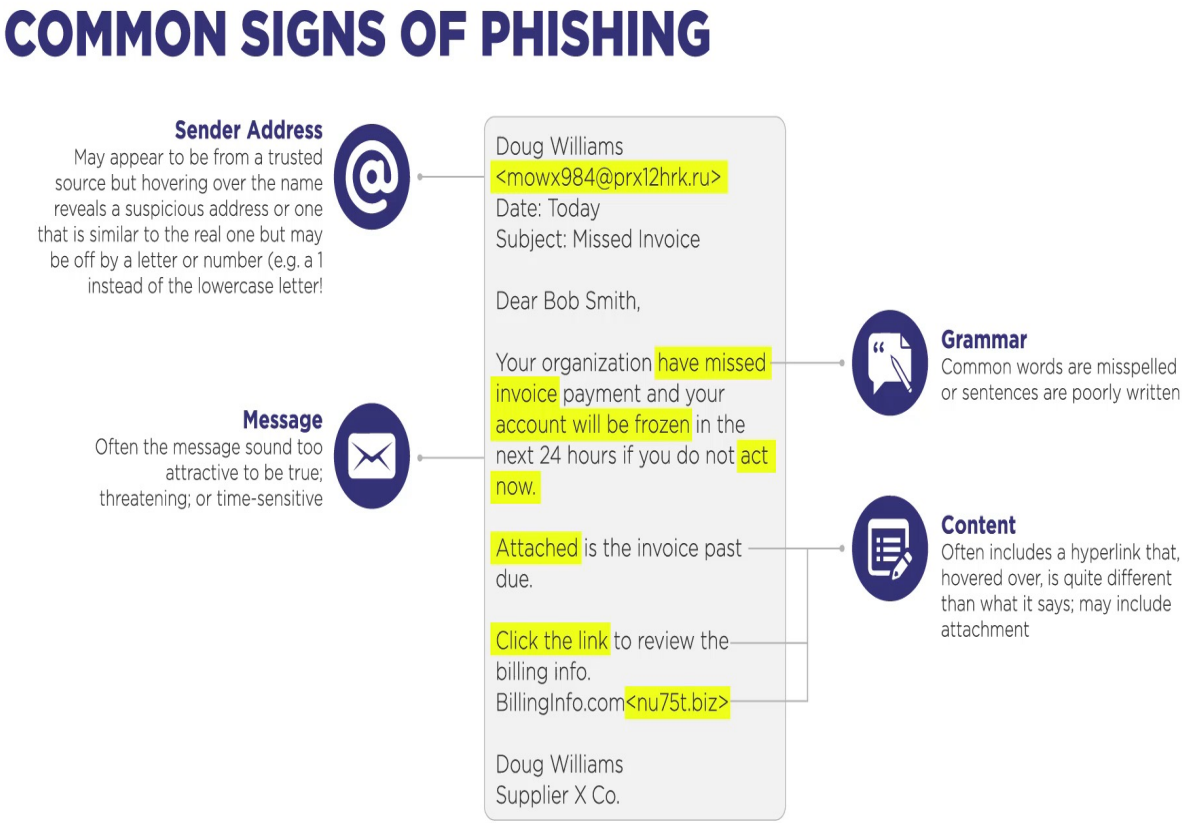
Phishing, Spearphishing & Whaling

Plenty of targets to choose from



Common Signs of Phishing

What to look for



Cyber Security Training and Consulting LLC

RETURN STRONGER

Ransomware: Resilience via backups

Backup Types

- Full
- Incremental
- Continuous Data Protection (Real-time)

Local and/or Cloud

Q&A