



ARIZONA
SMALL
BUSINESS
BOOT CAMP &
COLLECTIVE



RESPOND → PLAN → RETURN STRONGER

Holiday Hacking

PRESENTED BY

Jeffrey Crump & Chris Alexakis



Copyright

Copying, reproduction, reuse, modification, distribution, display, or transmission of any of the contents of this presentation for any purpose without the prior written consent of Cyber Security Training and Consulting LLC is strictly prohibited.

Copyright Disclaimer under Section 107 of the Copyright Act of 1976, allowance is made for “fair use” for purposes including criticism, comment, news reporting, teaching, scholarship, and research. Fair use is permitted by copyright statute that might otherwise be infringing.

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

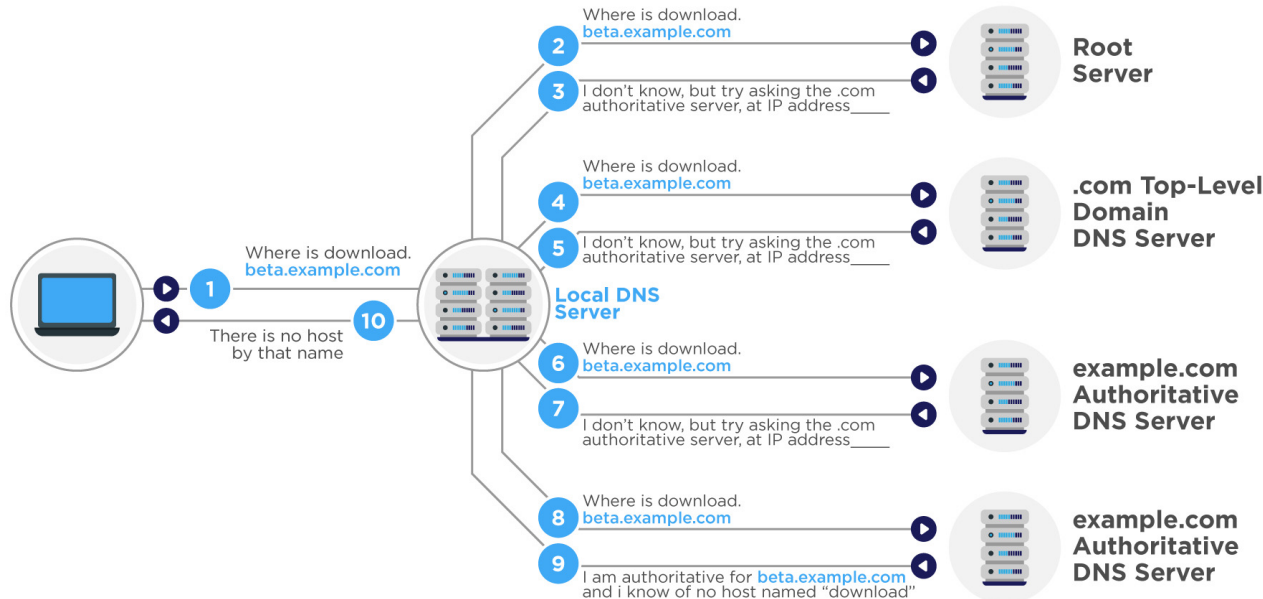
Ransomware

- Building resilience



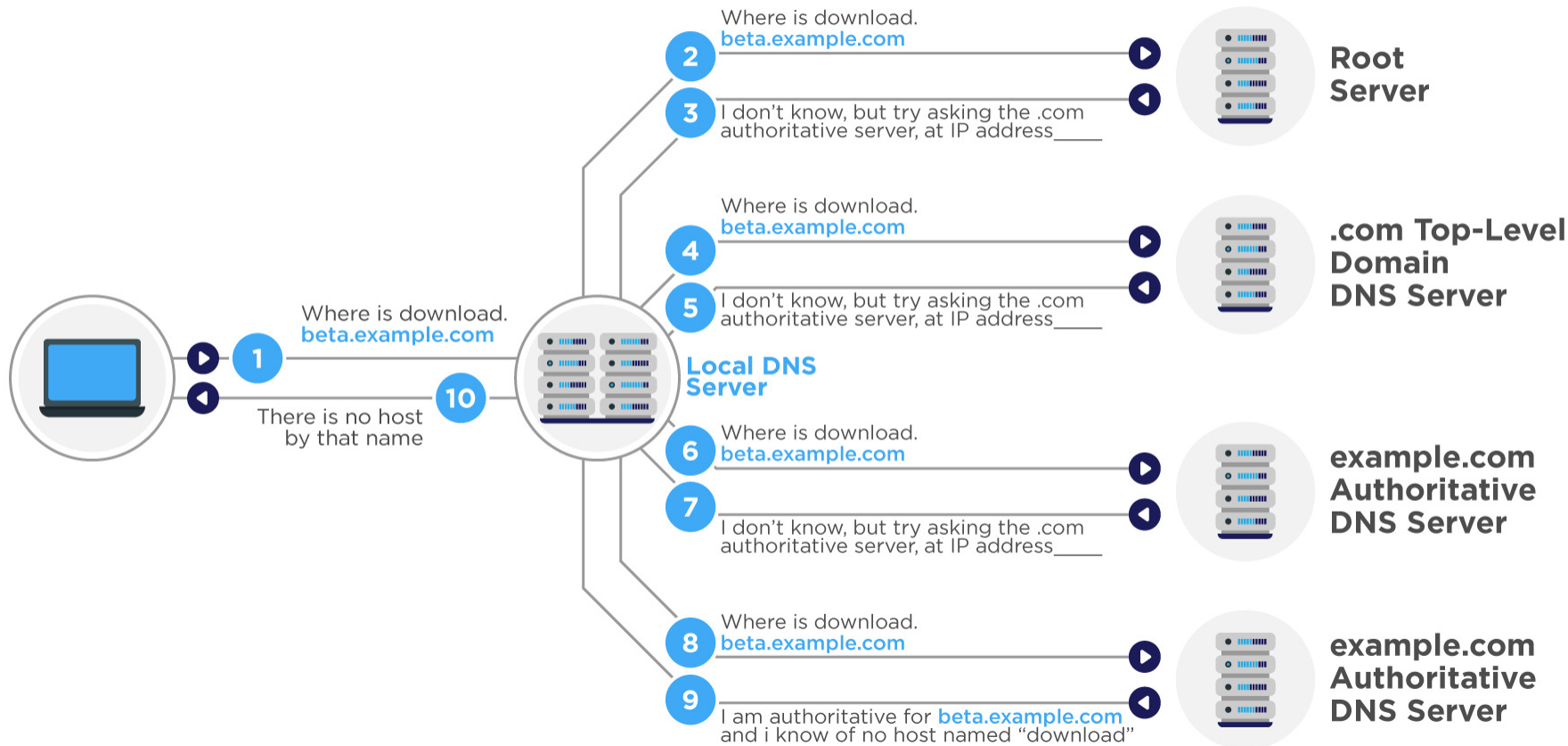
Spoofing: Website

HOW DNS WORKS



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

HOW DNS WORKS



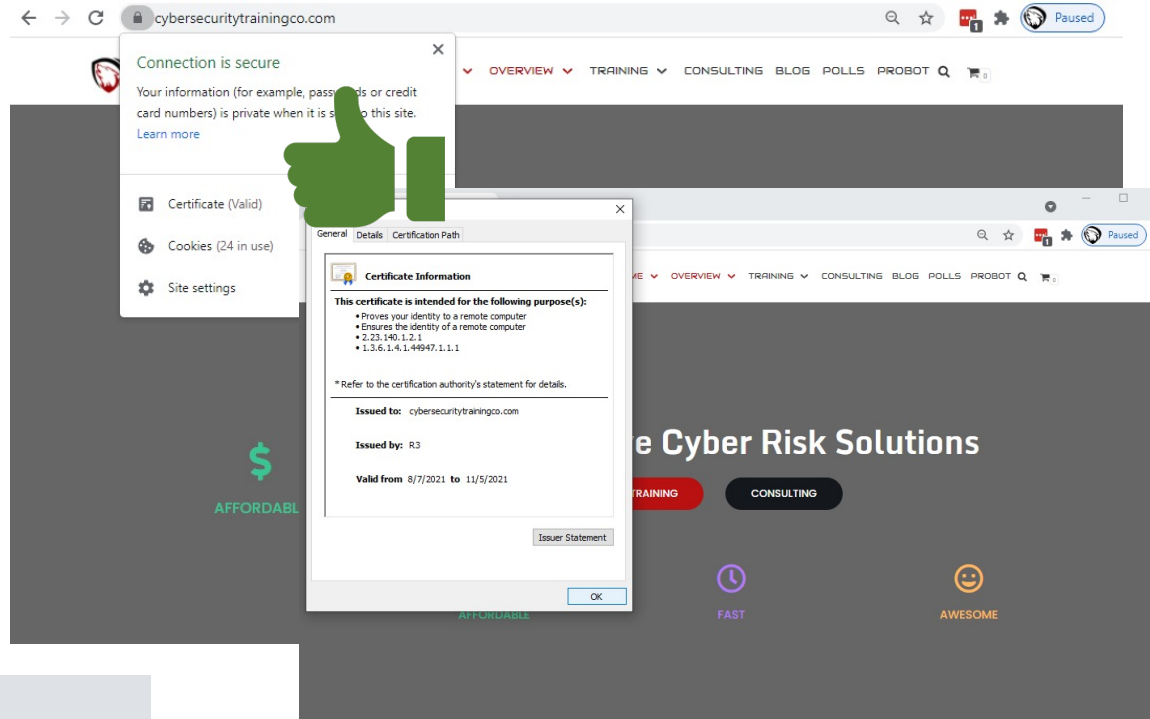
Spoofing: Website

Site Certificates

- Purpose
- Certificate Authorities (CAs)

Live Demonstration: Installing a website certificate

- GoDaddy
- Siteground



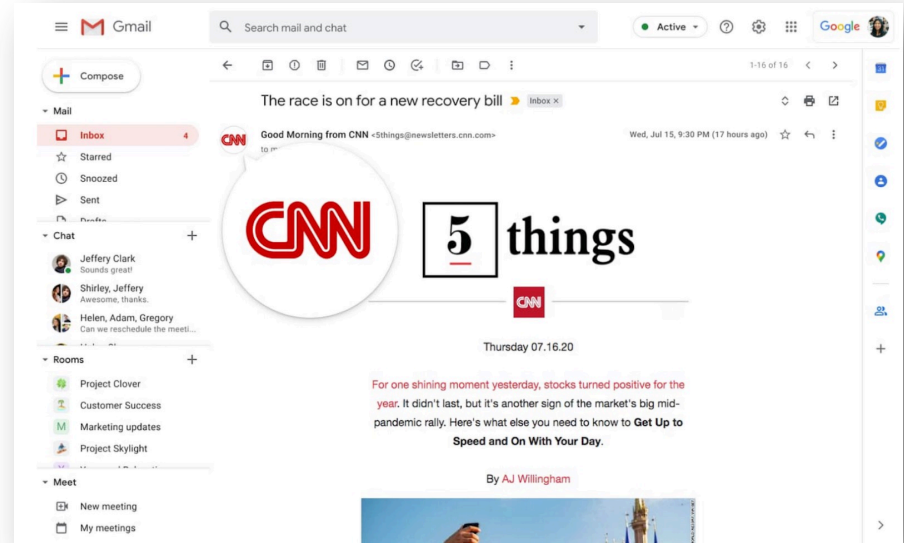
LIVE DEMONSTRATION

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

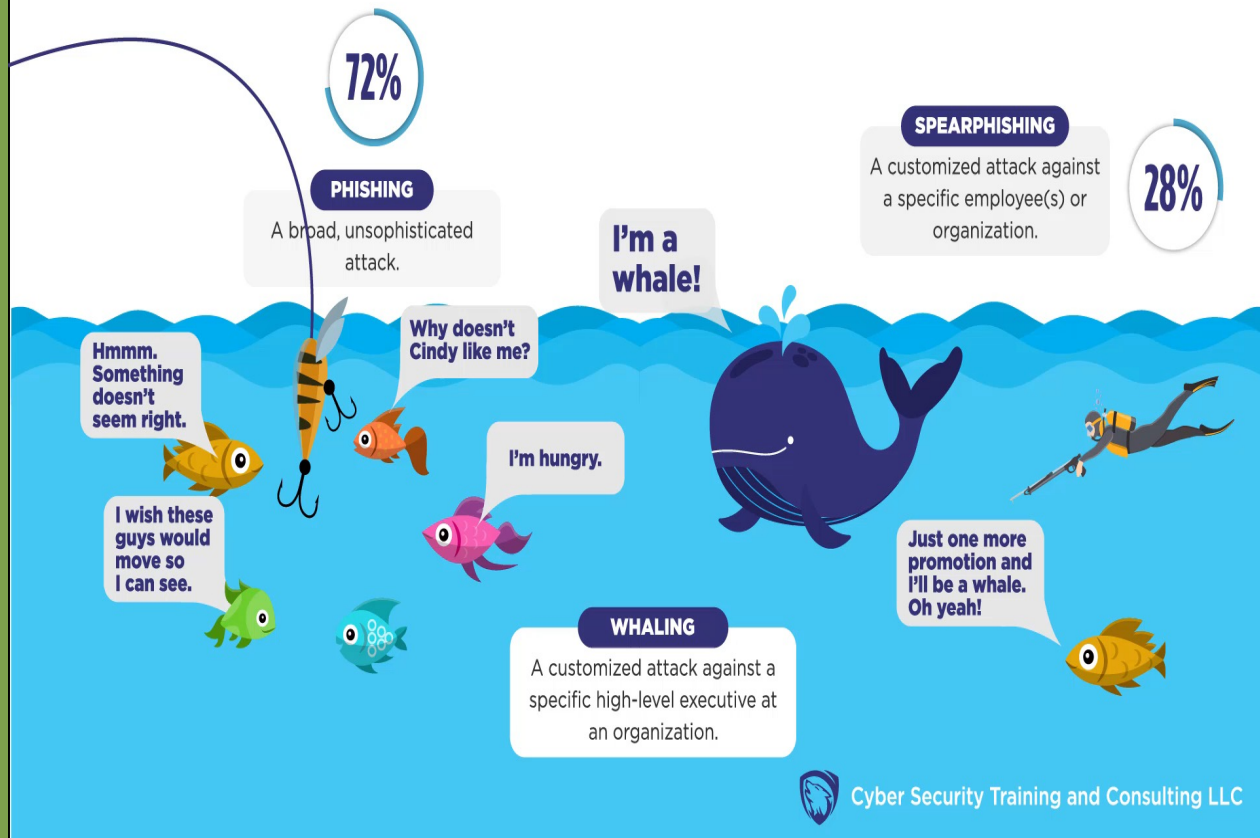


LIVE DEMONSTRATION

Phishing, Spearphishing & Whaling

Plenty of targets to choose from

PHISHING, SPEARPHISHING, AND WHALING



Common Signs of Phishing

What to look for

COMMON SIGNS OF PHISHING

Sender Address

May appear to be from a trusted source but hovering over the name reveals a suspicious address or one that is similar to the real one but may be off by a letter or number (e.g. a 1 instead of the lowercase letter!



Doug Williams
<mowx984@prx12hrk.ru>
Date: Today
Subject: Missed Invoice

Message

Often the message sound too attractive to be true; threatening; or time-sensitive



Dear Bob Smith,

Your organization have missed invoice payment and your account will be frozen in the next 24 hours if you do not act now.

Attached is the invoice past due.

Click the link to review the billing info.
BillingInfo.com<nu75t.biz>

Doug Williams
Supplier X Co.



Grammar

Common words are misspelled or sentences are poorly written



Content

Often includes a hyperlink that, hovered over, is quite different than what it says; may include attachment



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