Phishing and Account Compromise

CS563 / ECE524

Nikita Borisov, Spring 2026

Lecture Outline

- Phishing and Account Compromise
  - Goals
  - Approaches
  -

Phishing

- What is phishing?
- Have you been phished recently?
- Are you good at detecting phishing? What do you look for?

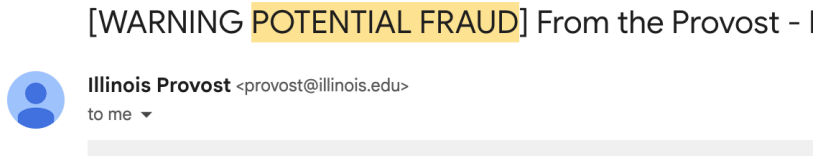
Modern Phishing Infrastructure

- What is needed for a successful phishing attack?
- Phishing email
  - Design, distribution
- Phishing website
  - Domain, hosting, design, credential capture
- Monetization
  - Direct abuse, lateral attacks, resale, more phishing

Commoditization

- Early security: single attacker performs end-to-end compromise / exploit
  - **Kits** provide software that automate compromise tasks
  - **Marketplaces** provide compromise services
- Specialists *commoditize* security vulnerabilities
  - Phish email design, malicious hosting, domain generation, …
- Phish markets
  - Sell compromised accounts
- Vertical integration
  - Phishing-as-a-Service

Defending from Phishing



- Email security: minimize threat of spoofed email
  - DKIM/DMARC
- Email scanning: find/block suspicious emails, scan attachments / links
  - Spam filters, ProofPoint, Barracuda
- Browser defenses: identify suspicious web pages, blacklist hosts, highlight potential brand impersonation
  - Chrome SafeBrowsing
- User training: education, fake phishing campaigns

Why is Detection Hard?

- Constantly evolving attacks
  - New text, new vectors (attachments, zip files, google doc, email rendering, …)
  - Polymorphism
- Attackers have access to detection tools
- User training has questionable value

Risk-Based Authentication

- Assign *risk factors* to each authentication attempt
  - Require extra authentication (email/SMS/…) for more risky logins
  - Report risky behavior to users / security teams
  - In the limit, deny authentication altogether
- What are costs / benefits of this?
- What are the risk factors?

Risk Factors

- IP address / geolocation
  - Location consistency: does it make sense for this user?
  - Location reputation: do attacks often come from here?
- Device / browser fingerprinting: user consistency and automation detection
- User activity: time of day, biometrics, types of activity
- Attack detection: login fits patterns of attack campaigns
- How secure are these?
- How can these be reconciled with privacy?

Attack Compromise Detection

Last account activity: 1 minute ago
Open in 1 other location · Details

- Account Security Interfaces
  - Expose account activity to users
- Compromised Account Detection
  - Notify users of suspicious activity
  - Force re-authentication, password change, account recovery

Machine Learning in Phishing

- Big reliance on learning in detection
  - Identify suspicious email, websites, domains, activity
- ML innovation quickly adopted
  - Feature-based classifiers -> deep learning -> LLMs
- Scale a *big* issue
  - False positives and false negatives highly costly

Un-phishable Credentials

- Passwords are:
  - Static, portable, reusable
- Multi-factor authentication
  - SMS, Authenticator, Duo, security key
  - Proxy attacks, “MFA fatigue”
- Passkeys
  - Non-portable (double-edged!)

Perspective

- Phishing is three decades old. Why haven’t we solved it?
- Will we still be dealing with phishing in a decade or three?

Lecture 1

Phishing

Jan 29

Phishing and Account Compromise

Readings:

Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale

Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn — USENIX Security 2020

Catching Phishers By Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection

Hugo Bijmans, Tim Booij, Anneke Schwedersky, Aria Nedgabat, and Rolf van Wegberg — USENIX Security 2021

Lecture 2

Phishing Detection

Feb 3

Phishing and Account Compromise

Readings:

Less Defined Knowledge and More True Alarms: Reference-based Phishing Detection without a Pre-defined Reference List

Ruofan Liu, Yun Lin, Xiwen Teoh, Gongshen Liu, Zhiyong Huang, Jin Song Dong — USENIX Security 2023

Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting

Xu Lin, Panagiotis Ilia, Saumya Solanki, and Jason Polakis — USENIX Security 2022

Presenter: Nikita Borisov

Lecture 3

User Compromise Notifications

Feb 5

Phishing and Account Compromise

Readings:

Account Security Interfaces: Important, Unintuitive, and Untrustworthy

Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, Thomas Ristenpart — USENIX Security 2023

"Who is Trying to Access My Account?" Exploring User Perceptions and Reactions to Risk-based Authentication Notifications

Tongxin Wei, Ding Wang, Yutong Li, Yuehuan Wang — NDSS 2025

Next Steps

- Start reading
- Volunteer for present / scribe
- Next lecture: reading / reviewing papers
  - **1pm start!!**
- Never too soon to start thinking projects!