Deconstructing the phishing campaigns that target Gmail users

Elie Bursztein
Google, @elie

Daniela Oliveira
University of Florida
@dseabraoliveira

with the help of many Googlers, University of Florida collaborators, and Natalie Ebner
Slides: https://elie.net/bh19
Twitter: @elie, @dseabraoliveira
Phished users are the most likely to have their Google account compromised

Likelihood to have your account compromised

Data breaches, phishing, or malware?: Understanding the risks of stolen credentials - CCS’17
What makes phishing an effective attack vector that is hard to mitigate?
Phishing is

- Evolving
- Targeted
- Well crafted
- Preventable
Phishing is an ever moving target
Everyday Gmail blocks over 100M+ phishing emails
Spear-phishing
Target specific individuals and organizations

Boutique phishing
Hand-crafted campaigns targeting a few dozen individuals or organizations

Bulk phishing
Automated campaigns targeting thousands of individuals and organizations
Cats through the ages

2000 BC

1200 AC

1800 AC

2020 AC
Drive phishing through the ages
68% of the phishing emails blocked by Gmail are different from day to day.
Phishing campaigns are short lived

- 7mn for boutique campaigns
- 13h for bulk campaigns
Phishing detection is hard as phishers quickly adapt their campaigns and keep the number of targeted users low.
Phishing is targeted
Phishing emails mostly targets businesses and non-profit.

Likelihood to be targeted by phishing:
- Company: 4.8x
- Non profit: 3.8x
- Gov related: 2.8x
- Edu: 2.1x
- Gmail
What phishing pages impersonate

- Email providers: 42%
- Cloud services: 25%
- Financial institution: 13%
- Ecommerce: 5%
- Delivery companies: 3.9%
Detecting advanced-phishing requires context that only the user has
Gmail inbox soft warnings help users decide which emails are phishing.
Why users end-up being phished?
45% of the Internet users don’t know what phishing is
Phishing is successful because it tricks the way our brain makes decisions.
Especially with regard to deception detection...
Interindividual Differences Impacting Deception Detection Abilities

- Cognitive motivation
- Dual-processing (System 1/System 2)
- Emotional Intelligence
- Brain functioning
- Hormones
- Personality
- Mood
Brain Dual-processing Mode

**System 1**
- Fast
- Automatic
- Uses mental shortcuts
- Intuitive
- Emotional
- Little effort

**System 2**
- Slow
- Deliberative
- Logical
- Brain-energy consuming
Socioemotional functioning

- Emotional intelligence
- Cognitive motivation
- Personality
- Mood
Neurobiology - Hormones

Decrease Deception Detection
- Testosterone/Estrogen
- steroid/sex hormones
- Oxytocin
  “social” hormone
- Serotonin/dopamine
  “feeling good” chemicals

Increase Deception Detection
- Cortisol
  “stress” hormone
Section 2

Phishing is well-crafted
Phishers add deceptive cues to messages to make them more appealing
Types of deceptive cues

- Persuasion
- Gain/Loss framing
- Emotional salience
Case-studies inspired from campaigns targeting Gmail users
Dear [CEO Name],

I hope this email finds you well. I am writing to discuss the progress of our upcoming contract. The conference was indeed valuable, as we were able to secure our first major contract, provided we have the system upgrades in place by next month.

Our usual contractor is willing to do us a solid and start working on the upgrade first thing tomorrow. However, they require proof of advance payments for the equipment before proceeding. This is why I am counting on you to pay the invoice as soon as it hits your inbox. Please send me the wire receipt as soon as it is done so I can share it with our contractor.

Reed Black Ph.d
CEO of the Construction ABC

[CEO Name]
<ceo@constructionABC.com>
Due to a system error you were double charged for your last order, a refund process was initiated but could not be completed due to errors in your billing information.

REF CODE: 2550CGE

You are required to provide us a valid billing address. Click here to update your address.

After your information has been validated you should get your refund within 3 business days.

We hope to see you again soon.

Amazin.com
Email ID: 00981182
CALIFORNIA WILDFIRE RELIEF FUND

To help all of those affected by the California wildfires, we are currently accepting donations. All payment methods will be accepted.

As part of our relief efforts, Google will match 50% of all contributions - for those making a contribution using Google Pay, we will match 100%. All proceeds will be used for rebuilding and providing individuals with food, shelter, and supplies.

Even if you’re not in the position to make a donation, we ask that you pass this message along. In a time like this, every bit helps.

DONATE

LET’S DO OUR PART, WHILE WE STILL CAN

The Google Family
User awareness is critical to mitigate phishing effectiveness.
Section 4
Phishing is preventable
Phishing key in-depth defenses

- Two factors authentication
- Education
- Detection (AI)
- Warnings
Not all 2FA technologies are equal

<table>
<thead>
<tr>
<th>Security level</th>
<th>Secondary email</th>
<th>SMS verification</th>
<th>Device prompt</th>
<th>Security key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boutique phishing</td>
<td>68%</td>
<td>96%</td>
<td>99%</td>
<td>100%</td>
</tr>
<tr>
<td>Spear-phishing</td>
<td>53-100%</td>
<td>76%</td>
<td>90%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Evaluating Login Challenges as a Defense Against Account Takeover - WWW19
Takeaways

Phishing is hard to detect as it evolves quickly

Deception detection is affected by cognition, emotion, and neurobiology

Phishers are persuasion experts

45% of users don’t understand what phishing is

Education and awareness is key to drive 2FA adoption and help users spot phishing

Phishing is preventable with strong 2FA connected device or security keys
Together we can stop phishing by getting user to use two factor authentication and educating them about phishing tactics & risks

Slides: [https://elie.net/bh19](https://elie.net/bh19)
Twitter: @elie, @dseabraoliveira