



Deconstructing the phishing campaigns that target Gmail users

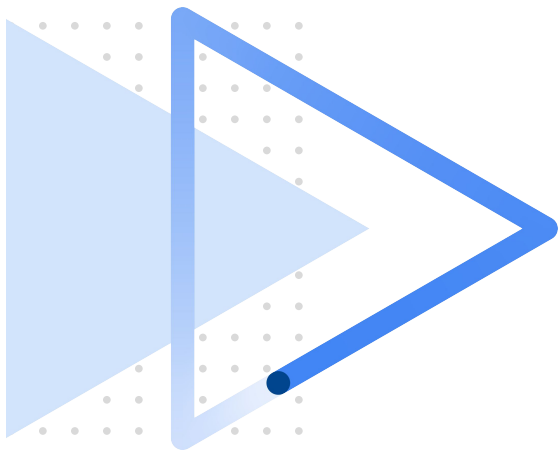


Elie Bursztein
Google, [@elie](#)



Daniela Oliveira
University of Florida
[@dseabraoliveira](#)

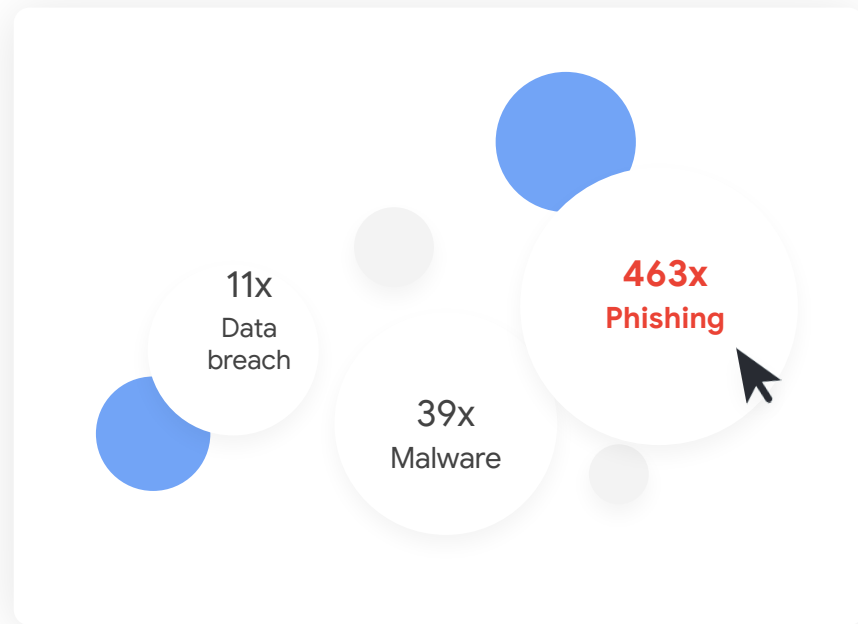
with the help of **many** Googlers, University of Florida collaborators, and Natalie Ebner



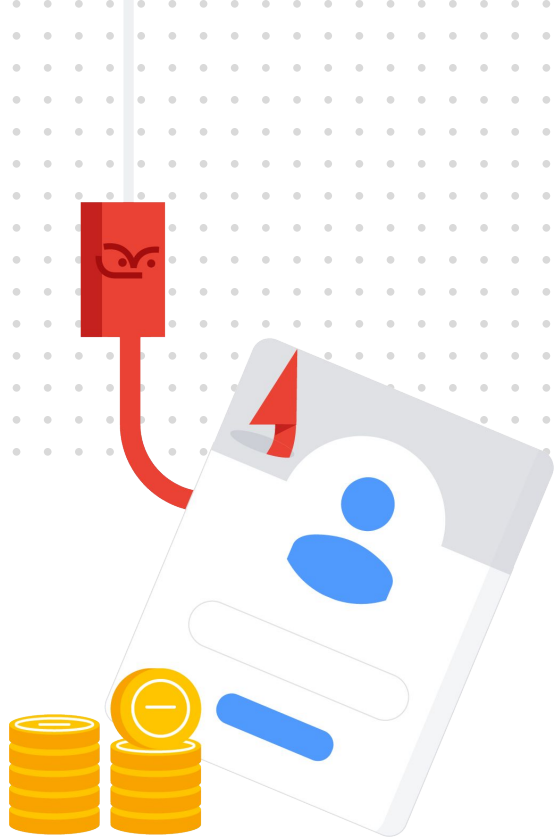
Slides: <https://elie.net/bh19>

Twitter: [@elie](#), [@dseabraoliveira](#)

Phished users are the most likely to have their Google account compromised

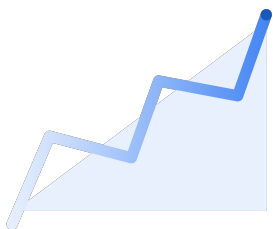


Likelihood to have your account compromised

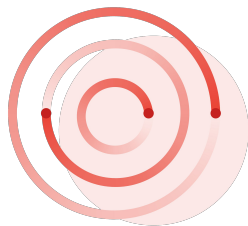


What makes phishing an effective attack vector that is hard to mitigate?

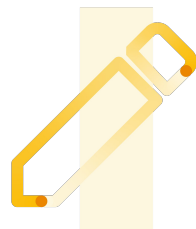
Phishing is



Evolving



Targeted



Well crafted



Preventable

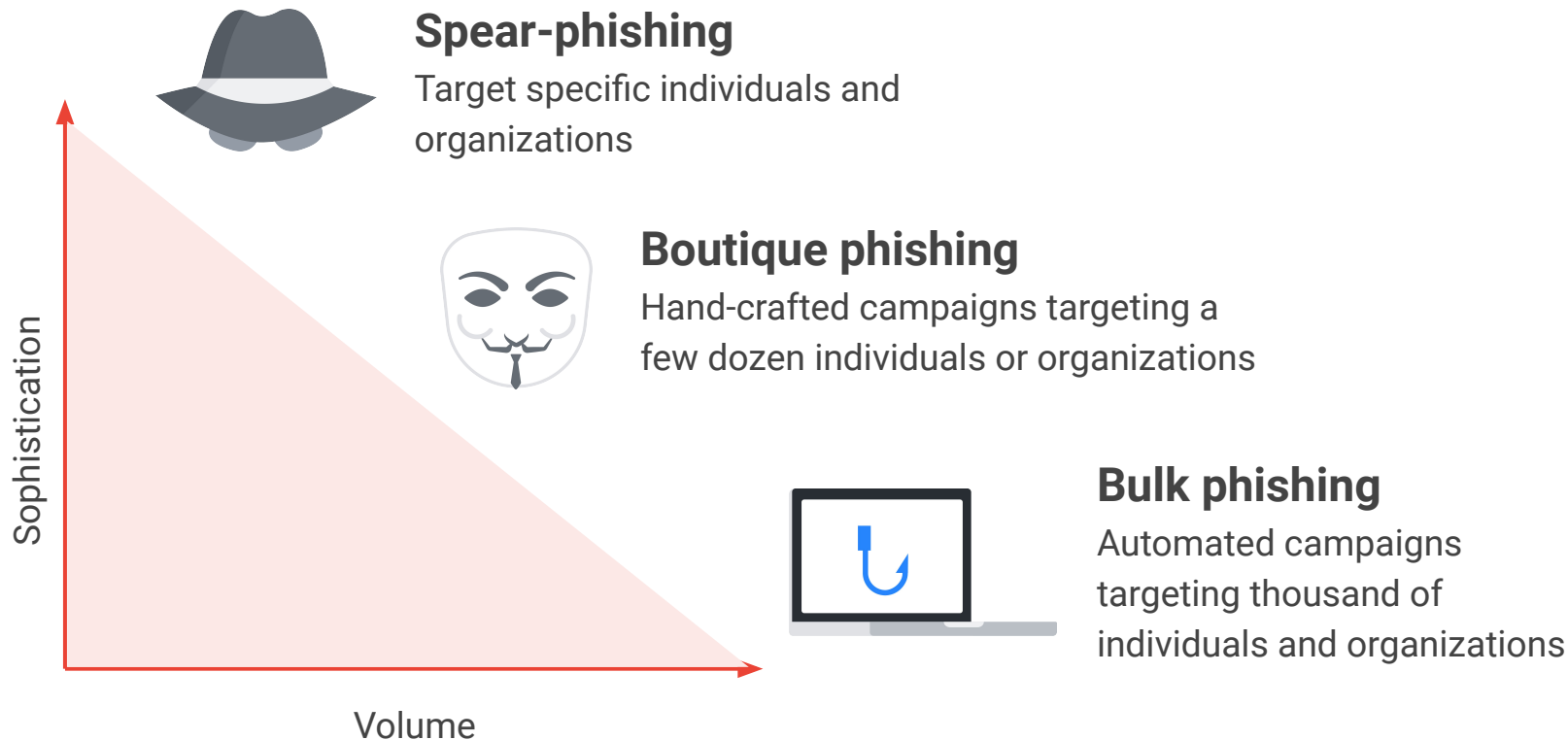


Phishing is an
ever moving target





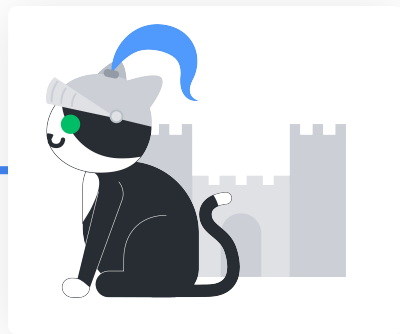
Everyday Gmail blocks over 100M+ phishing emails



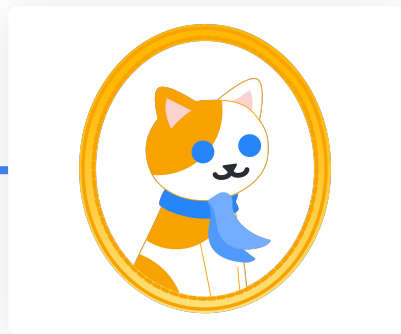
Cats through the ages



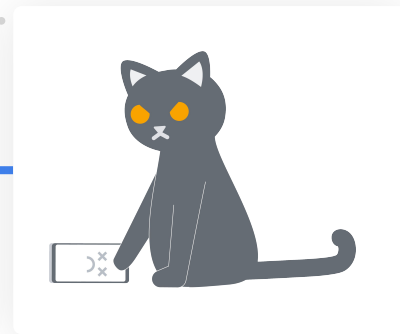
2000 BC



1200 AC



1800 AC



2020 AC

Drive phishing through the ages

Google Docs

Login your email address below to view the document.

Email Address

Email Password

Submit

To access our online secured documents page, you are required to login your email address. Unauthorized Access is prohibited.

The Intranet Website Management Center requires Internet Explorer 6.0 or greater

To View shared document you are required to Login with your email address below.

Google Docs

Ps AI Docs Excel Word OneNote Outlook PowerPoint Skype

Choose your email provider below and login:

YAHOO! Gmail

Windows Live AOL

Other emails

Google Drive

Keep everything. Share anything.

Keep everything. Share anything.

You have a Secure Document shared through our service To get access to this Document

[Click here to View](#)

Thank You for Using Google Document Sharing service!

©2014 Google - Terms of Service - Privacy Policy - Program Policies

Powered by Google

Welcome to Google Docs. Upload and Share Your Documents Securely

Sign in with your email address to view or download attachment.

Select your email provider

Gmail

Email

Password

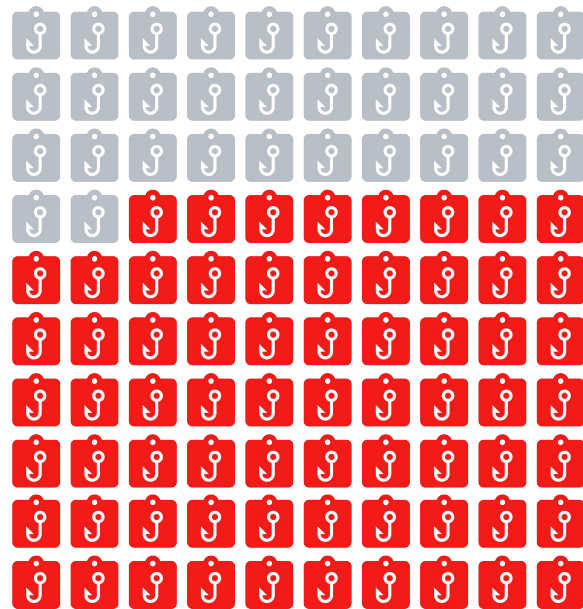
Sign in to view attachment

Stay signed in [Need help?](#)

Access your documents securely, no matter your location

68%

of the phishing emails
blocked by Gmail are
different from day to day



Phishing campaigns are short lived



7mn for boutique
campaigns



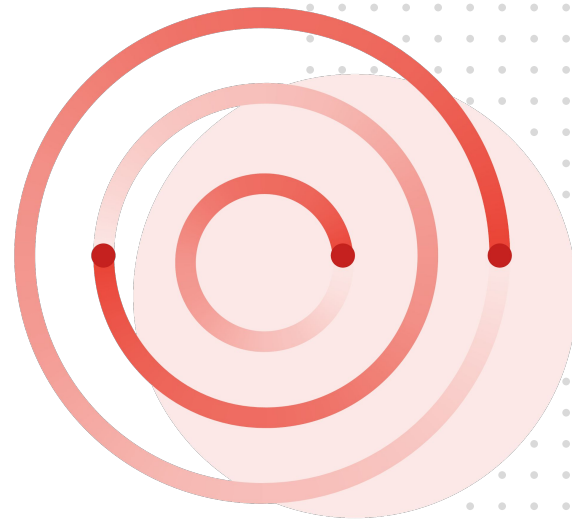
13h for bulk
campaigns

Phishing detection is hard
as phishers quickly adapt
their campaigns and
keep the number of
targeted users low

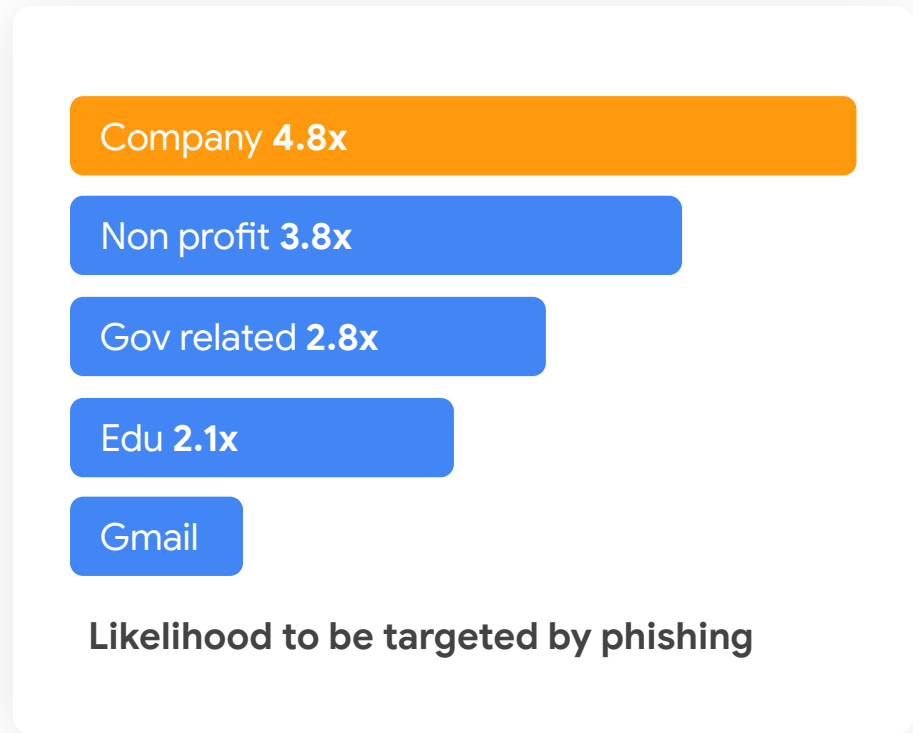




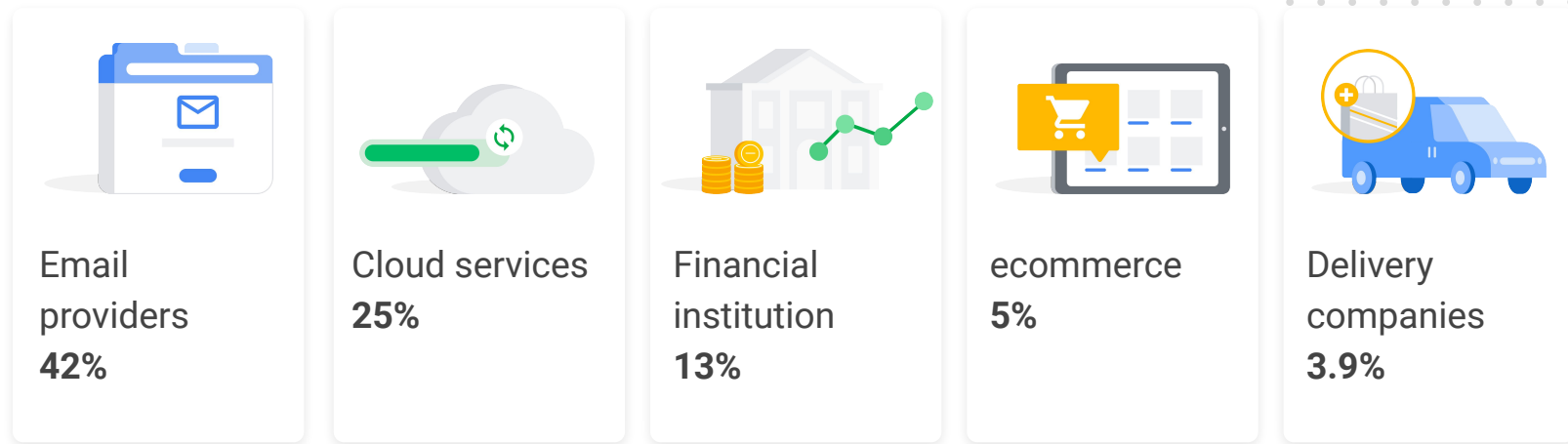
Phishing is targeted



Phishing emails
mostly targets
businesses
and non-profit



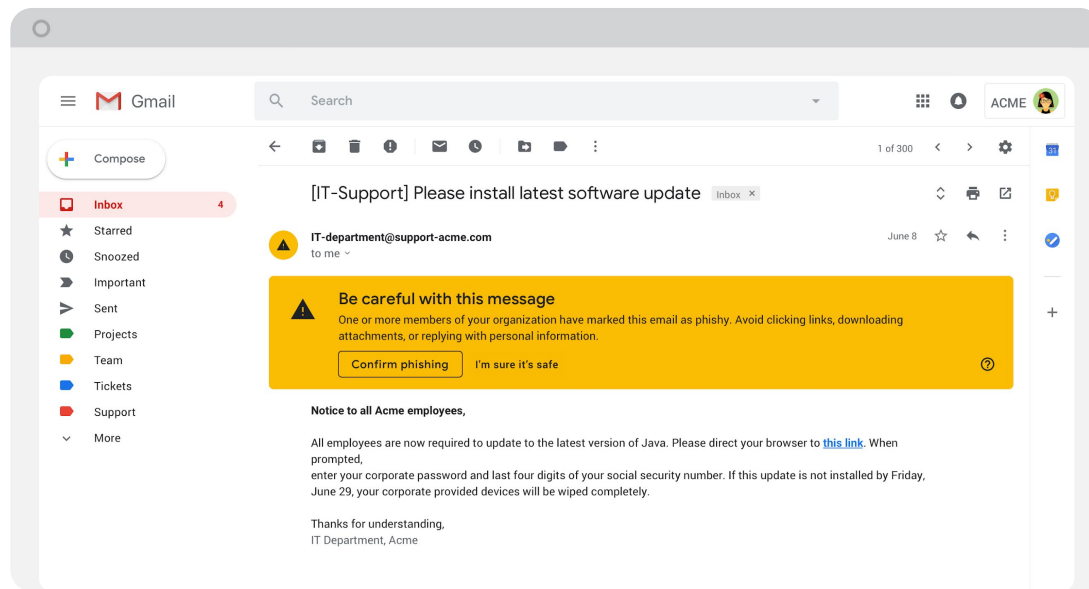
What phishing pages impersonate



**Detecting
advanced-phishing
requires context
that only the user has**



Gmail inbox soft warnings help users decide which emails are phishing

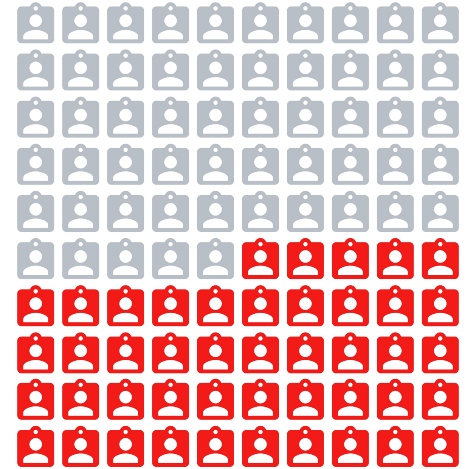




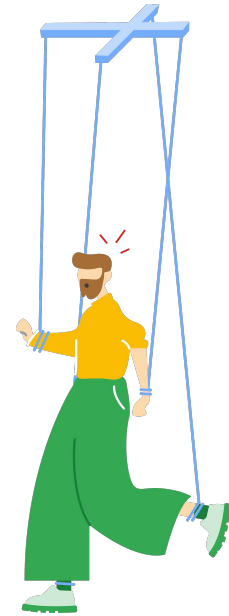
Why users end-up being phished?

45%

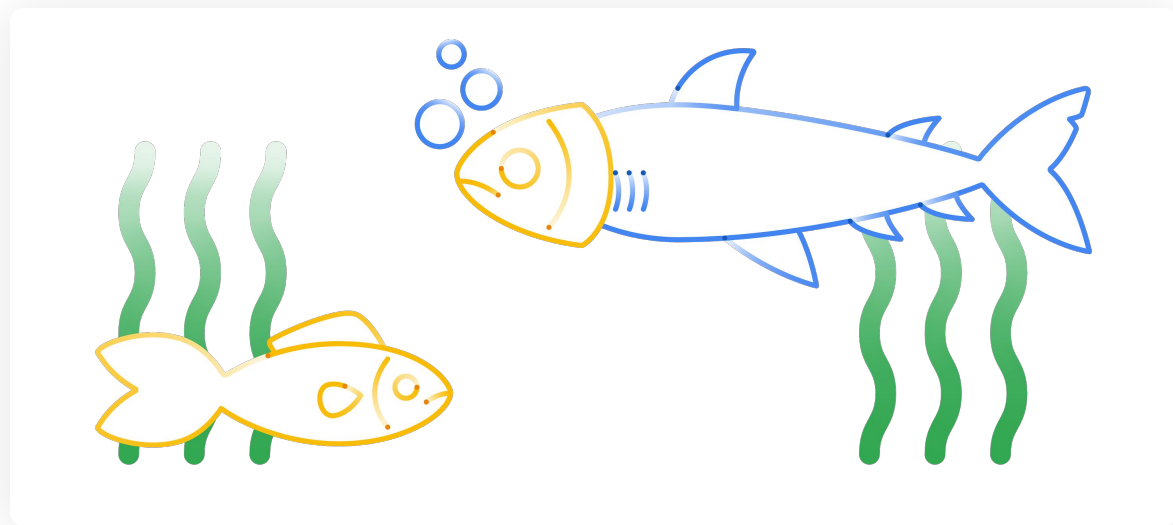
of the Internet users
don't know what phishing is



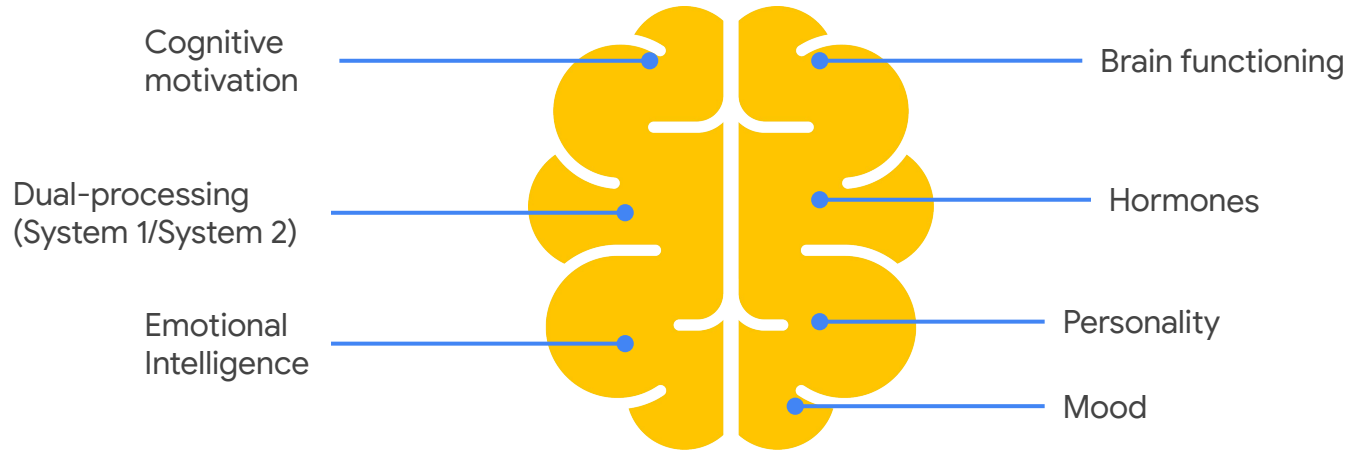
Phishing is successful
because it tricks the way
our brain makes decisions



Especially with regard to
deception detection...



Interindividual Differences Impacting Deception Detection Abilities

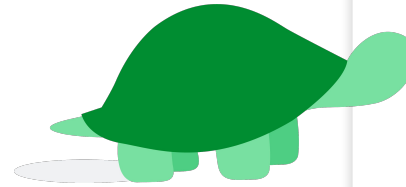


Brain Dual-processing Mode



System 1

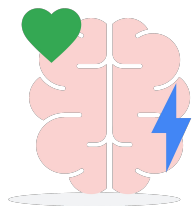
Fast
Automatic
Uses mental
shortcuts
Intuitive
Emotional
Little effort



System 2

Slow
Deliberative
Logical
Brain-energy
consuming

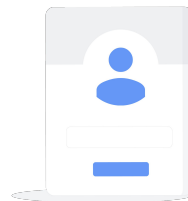
Socioemotional functioning



Emotional
intelligence



Cognitive
motivation

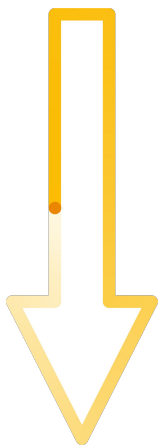


Personality



Mood

Neurobiology - Hormones

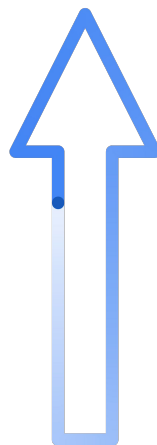


Decrease Deception Detection

Testosterone/Estrogen
steroid/sex hormones

Oxytocin
“social” hormone

Serotonin/dopamine
“feeling good” chemicals



Increase Deception Detection

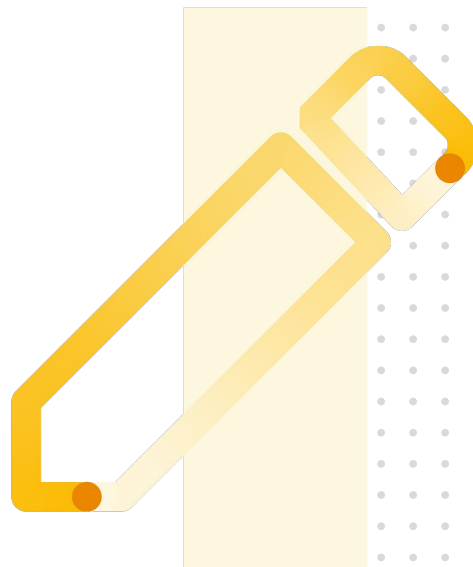
Cortisol
“stress” hormone





Section 2

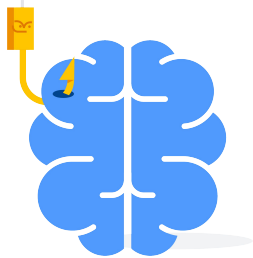
Phishing is well-crafted



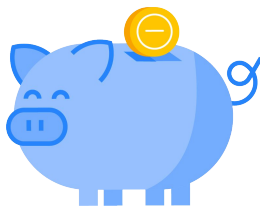
Phishers add deceptive cues to messages to make them more appealing



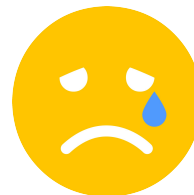
Types of deceptive cues



Persuasion



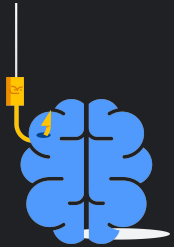
Gain/Loss
framing



Emotional
salience



Case-studies inspired
from campaigns
targeting Gmail users



Persuasion (Authority)

Google

The screenshot shows a Gmail interface in a browser window. The address bar displays 'http://mail.google.com'. The email header includes the sender's name 'CEO Name' with the email address '<ceo@constuctionABC.com>' and the time '3:05 PM (1 hour ago)'. The sender's profile picture is a yellow hard hat icon with the name 'ABC' below it. The email body contains three paragraphs of text. The first paragraph states that a conference was worth it because a major contract was secured, contingent on system upgrades by next month. The second paragraph explains that the contractor is ready to start work but requires advance payments for equipment. The third paragraph is a direct request for the invoice to be paid as soon as it arrives, with a request for a wire receipt to be shared with the contractor. The email is signed 'Reed Black Ph.d' and 'CEO of the Construction ABC'.

Need payment ASAP

CEO Name <ceo@constuctionABC.com> 3:05 PM (1 hour ago)

ABC

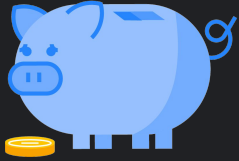
This conference was worth it! I was able to get our first major contract provided we have the system upgrades in place by next month.

Our usual contract is willing to do us a solid and start working on the upgrade first thing tomorrow but they want proof of advance payments for the equipment before jumping.

This is why I am counting on you to pay the invoice as soon as it hit your inbox. Please send me the wire receipt as soon it is done so I can share it with our contractor.

Reed Black Ph.d

CEO of the Construction ABC



Gain/Loss Framing (Loss)

Google

The screenshot shows a Gmail interface with a browser tab for 'Gmail' and a URL of 'http://mail.google.com'. The email is from 'Amazin <1234@amazin11.com>' to the user, received at 3:05 PM (1 hour ago). The subject is 'amazon Refund Notification'. The body text reads: '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'. At the bottom, there are buttons for 'Reply', 'Reply all', and 'Forward'.



Emotional Salience (Wildfire)

Google

A screenshot of a Gmail email interface. The browser address bar shows 'http://mail.google.com'. The email is from 'Google Relief <donations@relief-google.com>' to the recipient, dated 'Monday, November 19, 2018 8:16 AM'. The subject is 'California Wildfire Relief Funds'. The email body features the Google Pay logo and the heading 'CALIFORNIA WILDFIRE RELIEF FUND'. The text explains that Google is accepting donations to help with California wildfires and will match 50% of all contributions, or 100% for those using Google Pay. It also asks recipients to pass the message along if they cannot donate. A green 'DONATE' button is visible, followed by the text 'LET'S DO OUR PART, WHILE WE STILL CAN' and 'The Google Family'.

x Gmail x

← ↻ http://mail.google.com

☰ Gmail 🔍

+ 📧 ☆ 🕒 ▶ ▼

California Wildfire Relief Funds

Google Relief <donations@relief-google.com> to me Monday, November 19, 2018 8:16 AM ☆ ↶

Pay

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



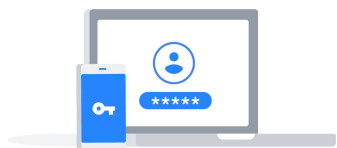


Section 4

Phishing is preventable



Phishing key in-depth defenses



Two factors
authentication



Education

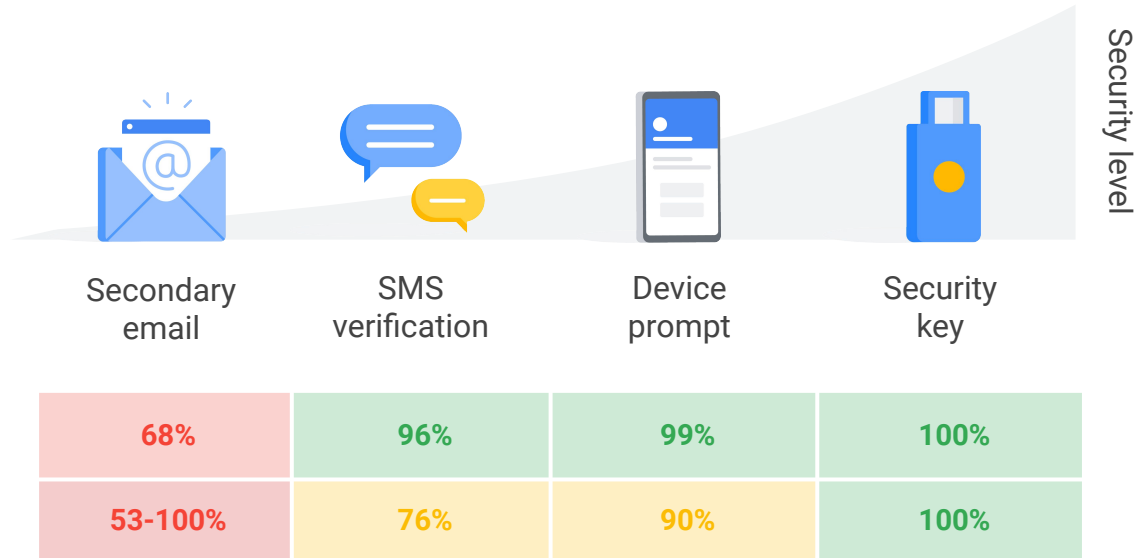


Detection (AI)



Warnings

Not all 2FA technologies are equal



Takeaways



Phishing is hard to detect as it evolves quickly



Deception detection is affected by cognition, emotion, and neurobiology



Phishers are persuasion experts



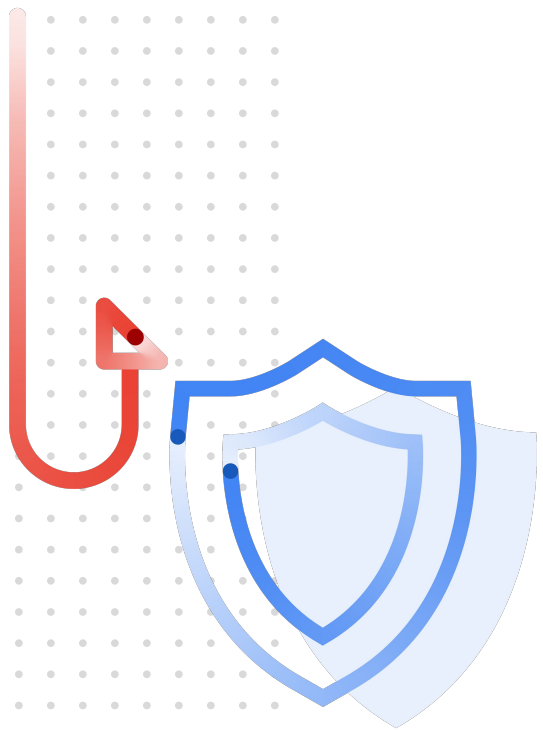
45% of users don't understand what phishing is



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>

Twitter: [@elie](#), [@dseabraoliveira](#)