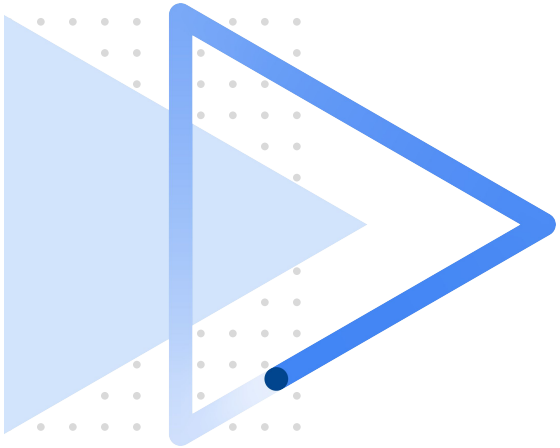
Google | UF

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

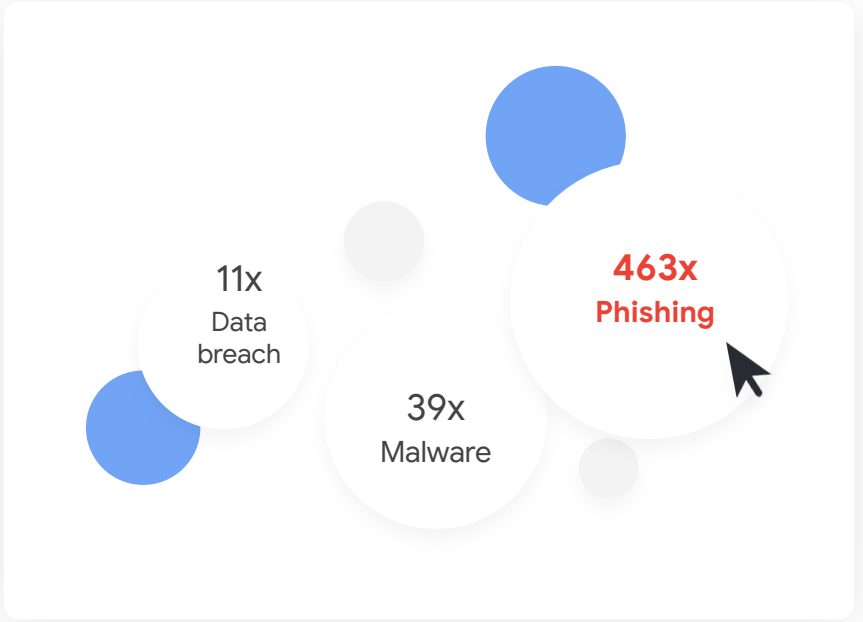


Slides: https://elie.net/bh19

Twitter: @elie, @dseabraoliveira

Google | UF

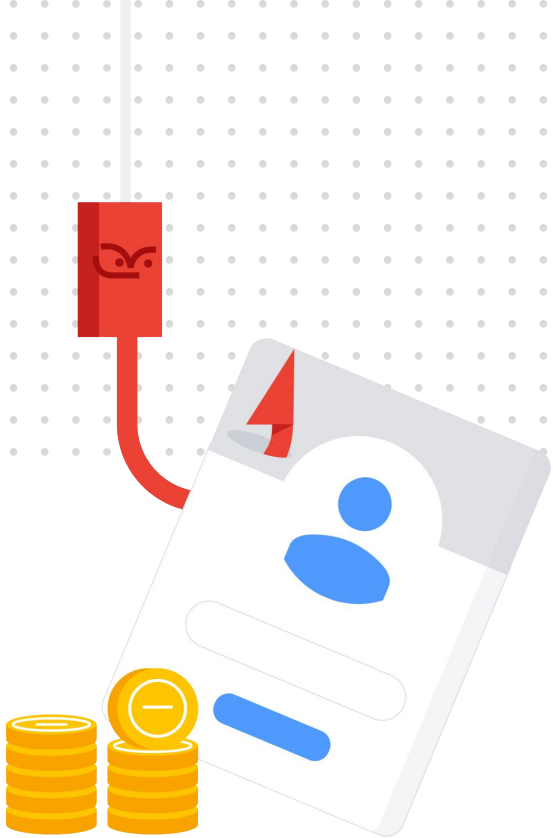
Phished users are the most likely to have their Google account compromised



Likelihood to have your account compromised

Google | UF

Data breaches, phishing, or malware?: Understanding the risks of stolen credentials - CCS'17

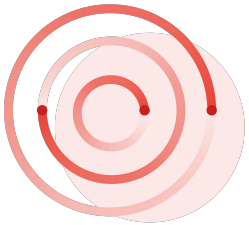


What makes phishing an effective attack vector that is hard to mitigate?

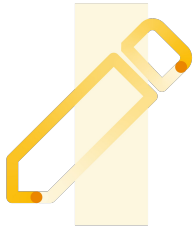
Google | UF

Phishing is

Evolving



Targeted



Well crafted

Preventable

Google | UF

Phishing is an ever moving target

Google | UF

Everyday Gmail blocks over 100M+ phishing emails

Google | UF

Spear-phishing

Target specific individuals and organizations

Boutique phishing

Hand-crafted campaigns targeting a few dozen individuals or organizations

Bulk phishing

Automated campaigns targeting thousand of individuals and organizations

Google | UF

Cats through the ages

2000 BC

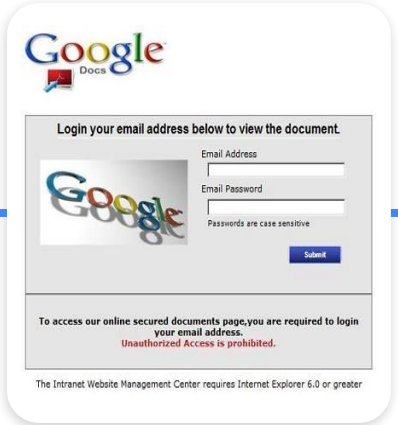
1200 AC

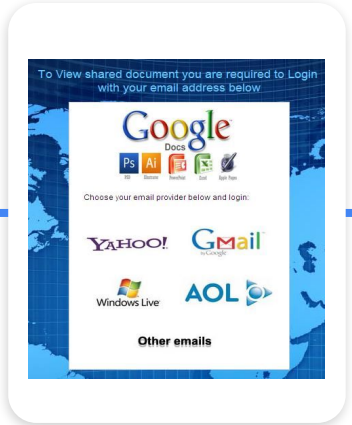
1800 AC

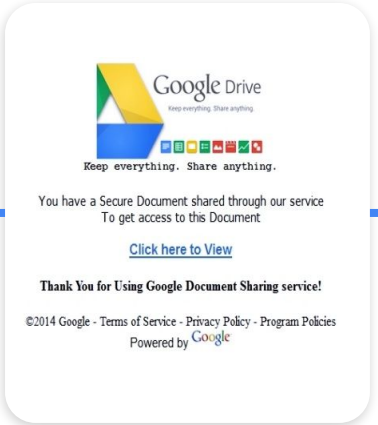
2020 AC

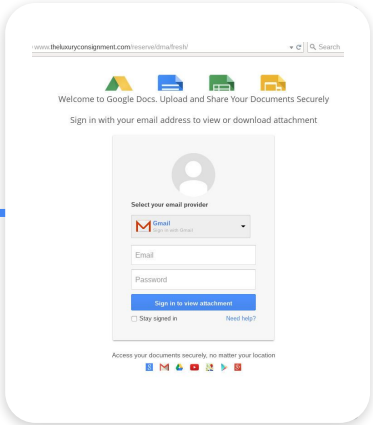
Google | UF

Drive phishing through the ages





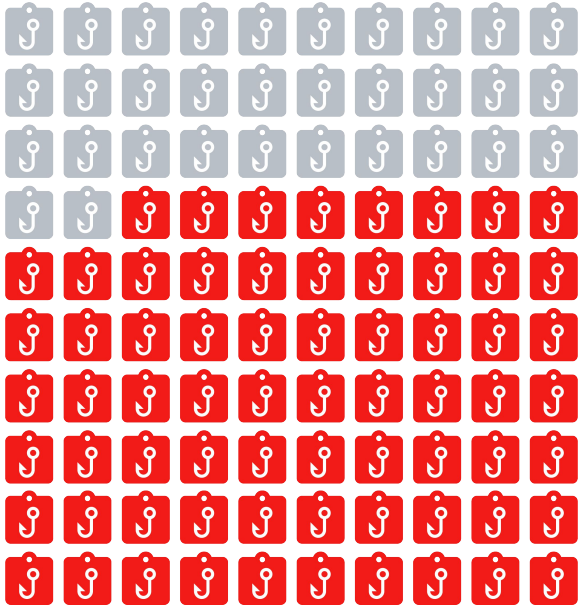




Google | UF

68%

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



Google | UF

Phishing campaigns are short lived

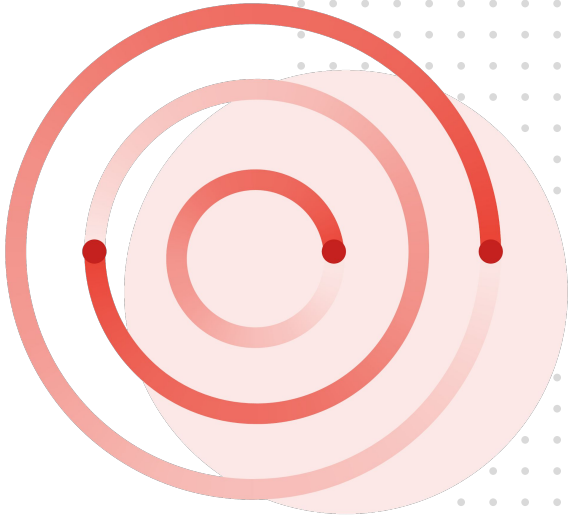
7mn for boutique campaigns

13h for bulk campaigns

Google | UF

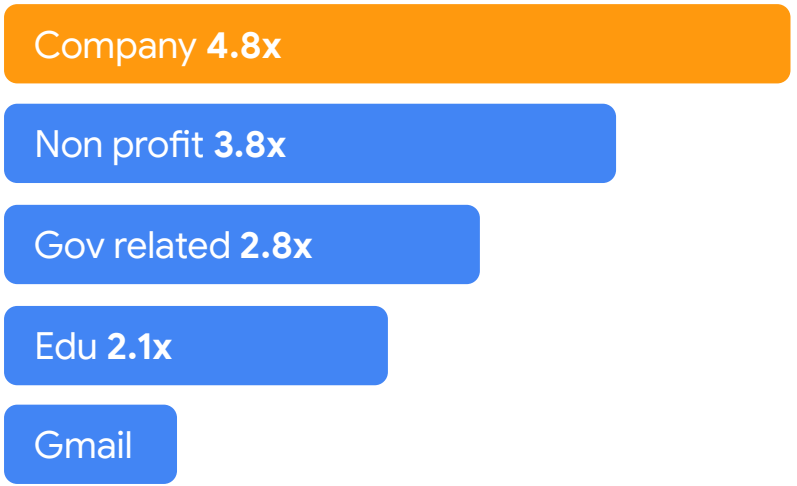
Phishing detection is hard as phishers quickly adapt their campaigns and keep the number of targeted users low

Phishing is targeted



Google | UF

Phishing emails mostly targets businesses and non-profit

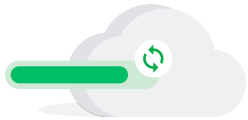


Likelihood to be targeted by phishing

Google | UF

What phishing pages impersonate

Email providers
42%



Cloud services
25%

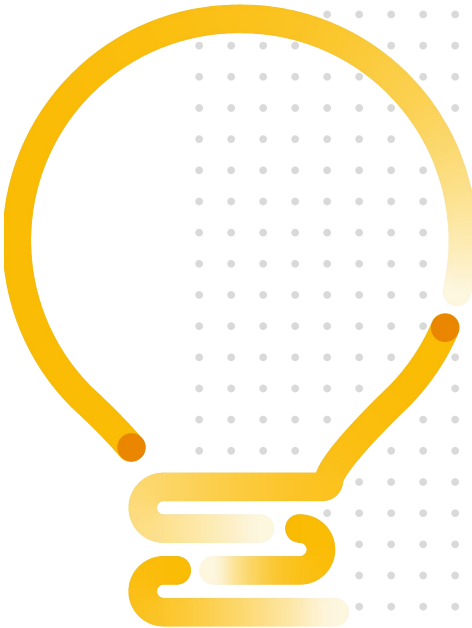
Financial institution
13%

ecommerce
5%

Delivery companies
3.9%

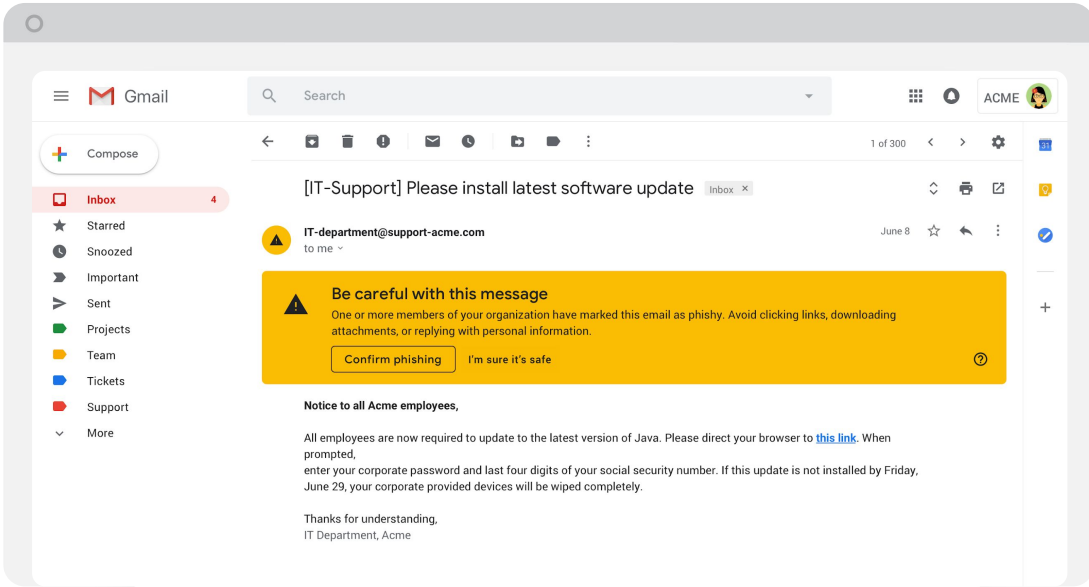
Google | UF

Detecting advanced-phishing requires context that only the user has



Google | UF

Gmail inbox soft warnings help users decide which emails are phishing



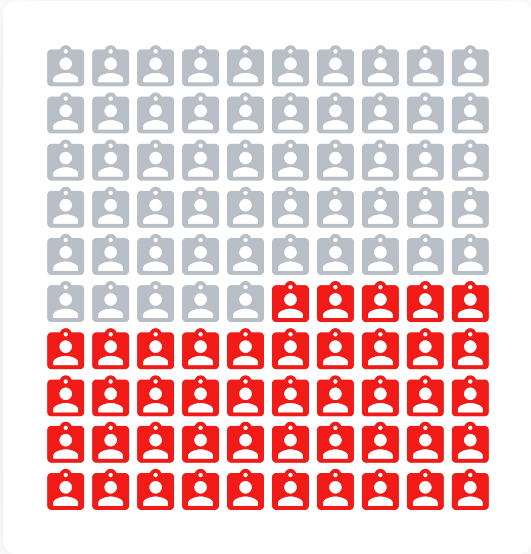
Google | UF

Why users end-up being phished?

Google | UF

45%

of the Internet users
don’t know what phishing is

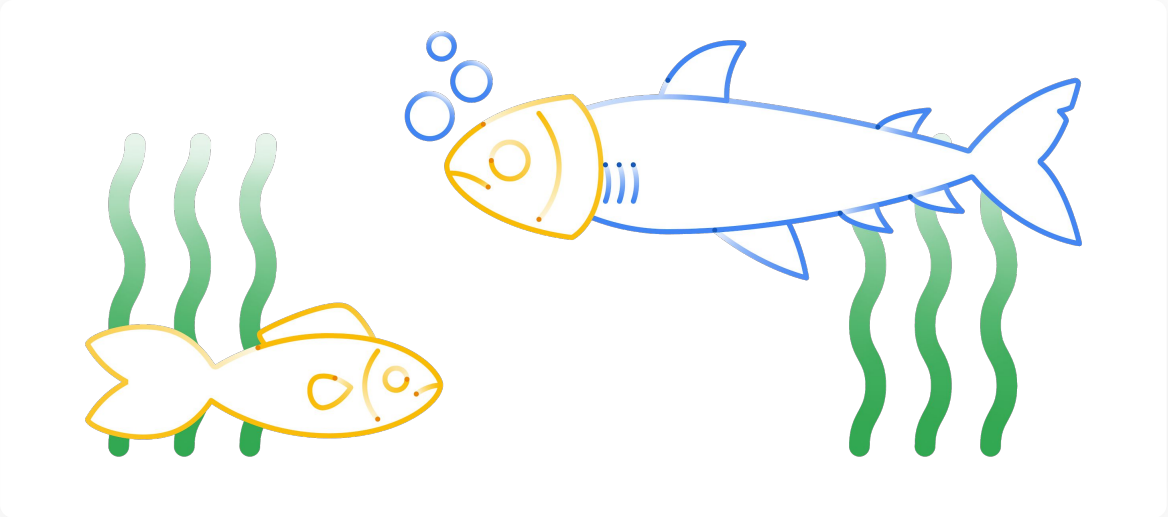


Google | UF

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

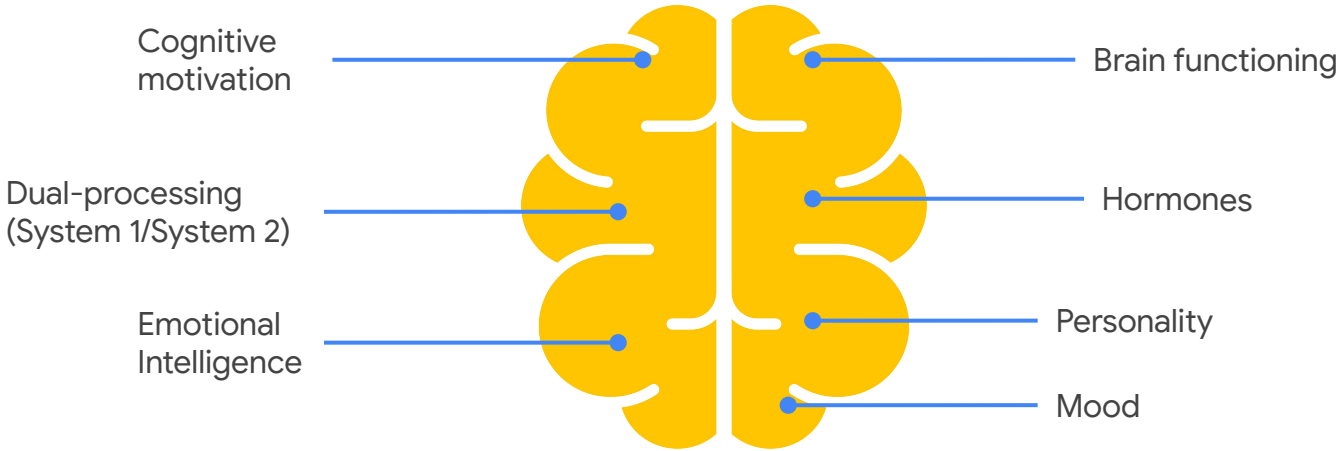
Google | UF

Especially with regard to deception detection...



Google | UF

Interindividual Differences Impacting Deception Detection Abilities

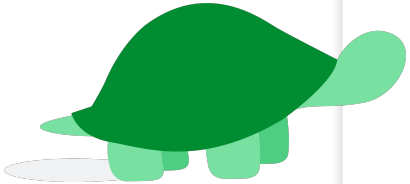


Google | UF

Brain Dual-processing Mode

System 1

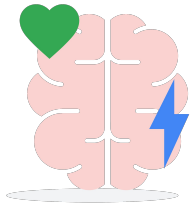
Fast
Automatic
Uses mental shortcuts
Intuitive
Emotional
Little effort



System 2

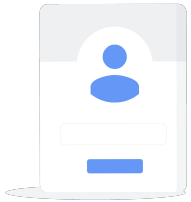
Slow
Deliberative
Logical
Brain-energy consuming

Socioemotional functioning



Emotional intelligence

Cognitive motivation

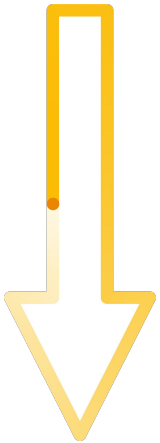


Personality

Mood

Google | UF

Neurobiology - Hormones

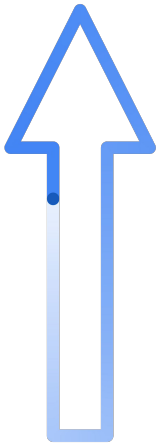


Decrease Deception Detection

Testosterone/Estrogen
steroid/sex hormones

Oxytocin
“social” hormone

Serotonin/dopamine
“feeling good” chemicals



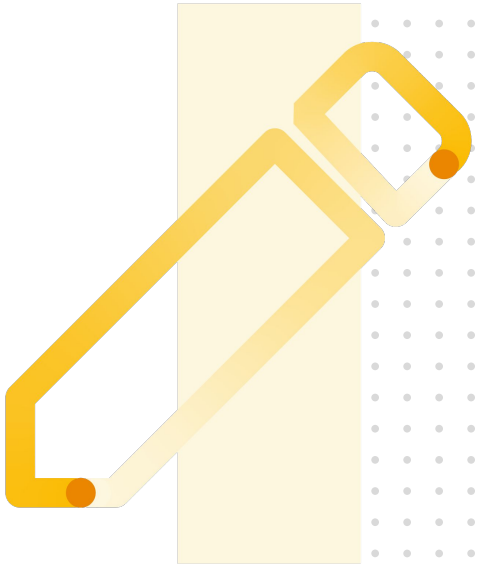
Increase Deception Detection

Cortisol
“stress” hormone

Google | UF

Section 2

Phishing is well-crafted

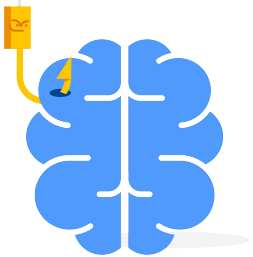


Google | UF

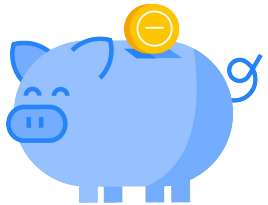
Phishers add deceptive cues to messages to make them more appealing

Google | UF

Types of deceptive cues



Persuasion



Gain/Loss framing

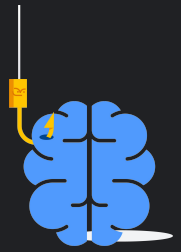
Emotional salience

Google | UF

Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing CHI'17

Case-studies inspired from campaigns targeting Gmail users

Google | UF



Persuasion (Authority)

Gmail

http://mail.google.com

Gmail

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

Google

Gain/Loss Framing (Loss)

Google

Gmail

http://mail.google.com

Gmail

You have a refund!

Amazin <1234@amazin11.com>
to me

3:05 PM (1 hour ago)

amazin **Refund Notification**

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

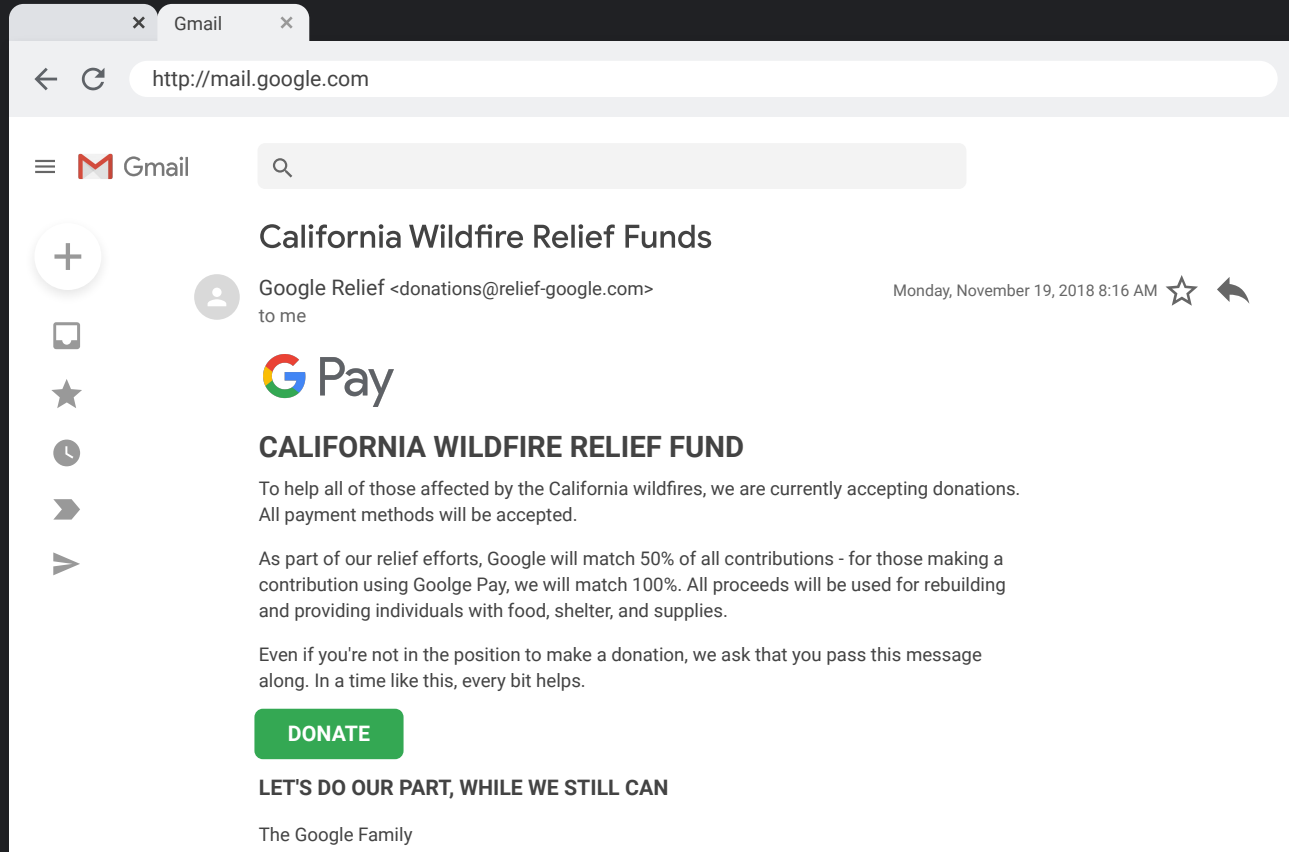
Click here to update your address

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

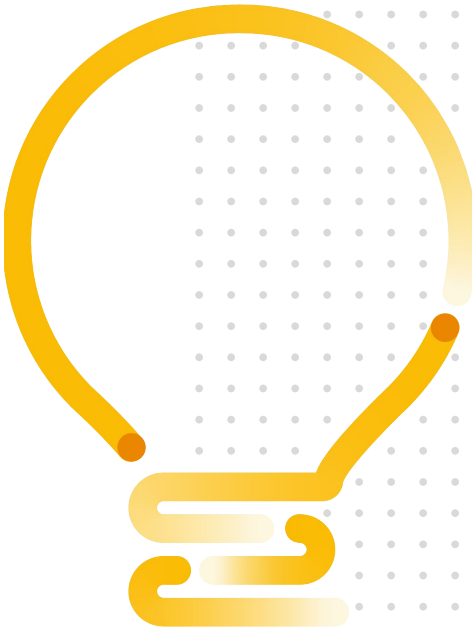
Reply | Reply all | Forward

Emotional Salience (Wildfire)



Google

User awareness is critical to mitigate phishing effectiveness



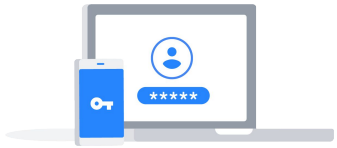
Google | UF

Section 4

Phishing is preventable

Google | UF

Phishing key in-depth defenses



Two factors authentication

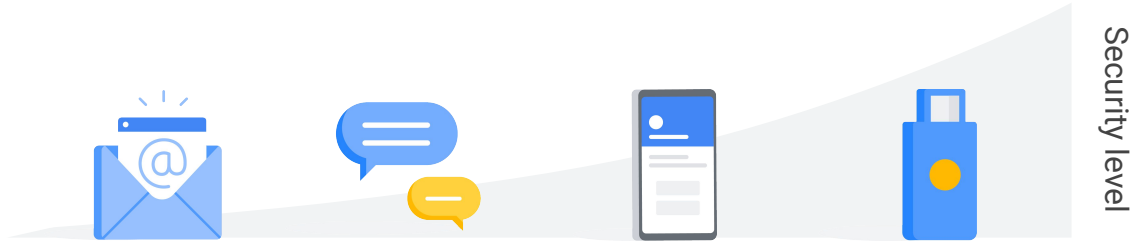
Education

Detection (AI)

Warnings

Google | UF

Not all 2FA technologies are equal



	Secondary email	SMS verification	Device prompt	Security key
Boutique phishing	68%	96%	99%	100%
Spear-phishing	53-100%	76%	90%	100%

Takeaways

Phishing is hard to detect as it evolves quickly

Deception detection is affected by cognition, emotion, and neurobiology

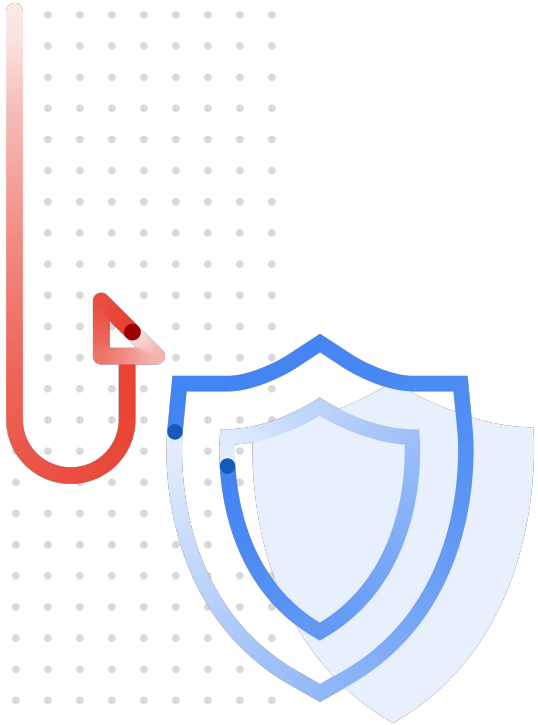
Phishers are persuasion experts

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

Google | UF



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

Google | UF