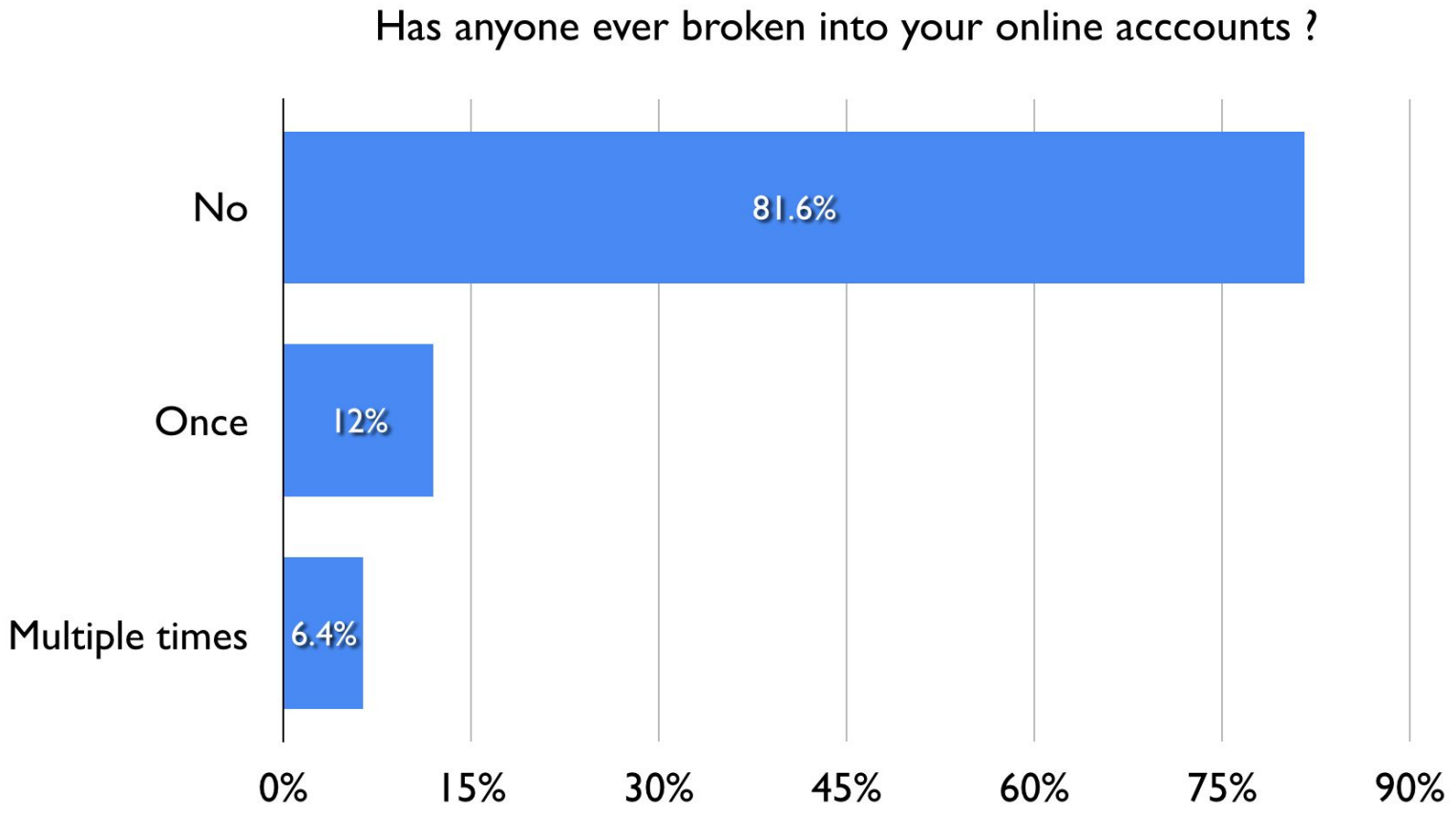
Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild

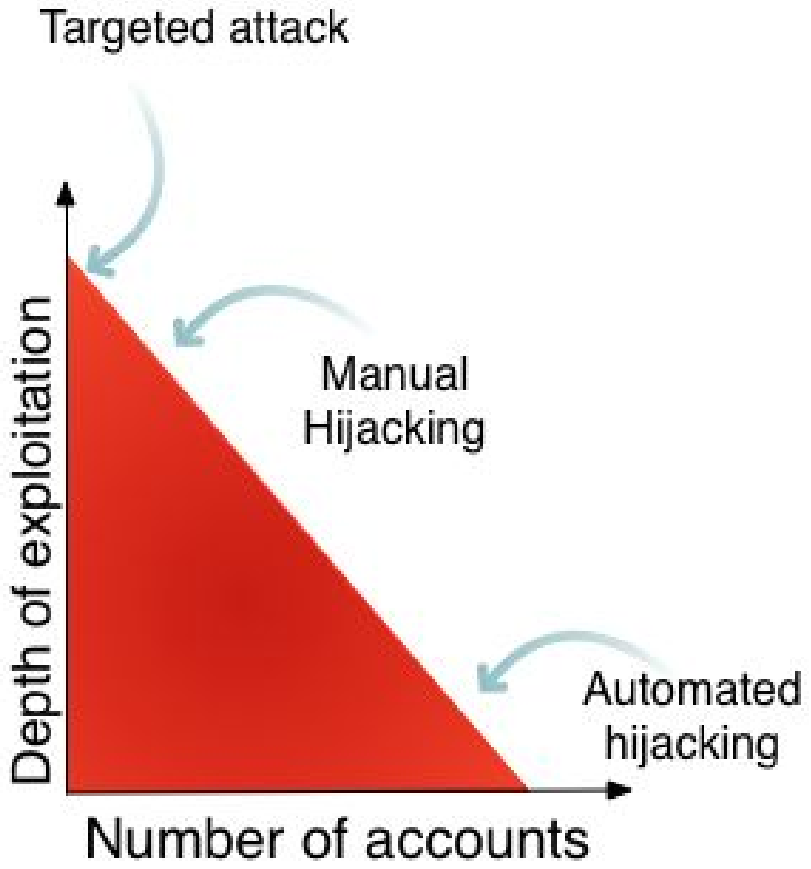
Elie Bursztein, Borbala Benko, Daniel Margolis, Tadek Pietraszek
Andy Archer, Allan Aquino, Andreas Pitsillidis (UCSD), Stefan Savage (UCSD)

Hijacking is a pervasive problem



10.000 US respondents - Survey run using Google consumers survey

Google's Hijackers Taxonomy



Automated hijacking

- High volume (millions)
- Automated tools
- Not much damage

Manual hijacking

- Low volume (at most low 1000s)
- Manual work,
- More damage to the account

Manual hijacker

- Professional scammer
- Follow a strict playbook
- Financially motivated
- Specialized in social engineering
- Knowledgeable but not tech savvy

Outline

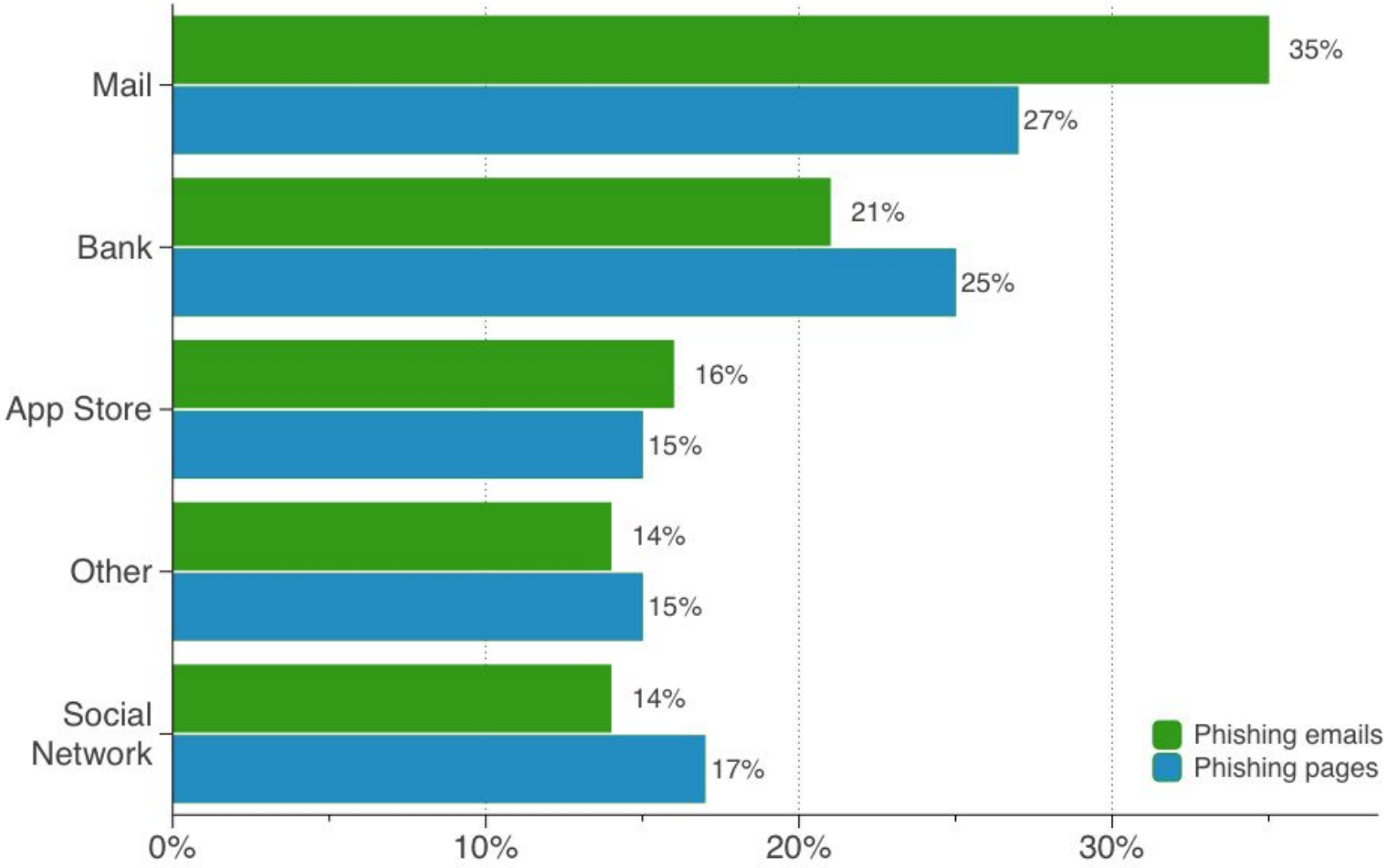
Credential theft

Account exploitation

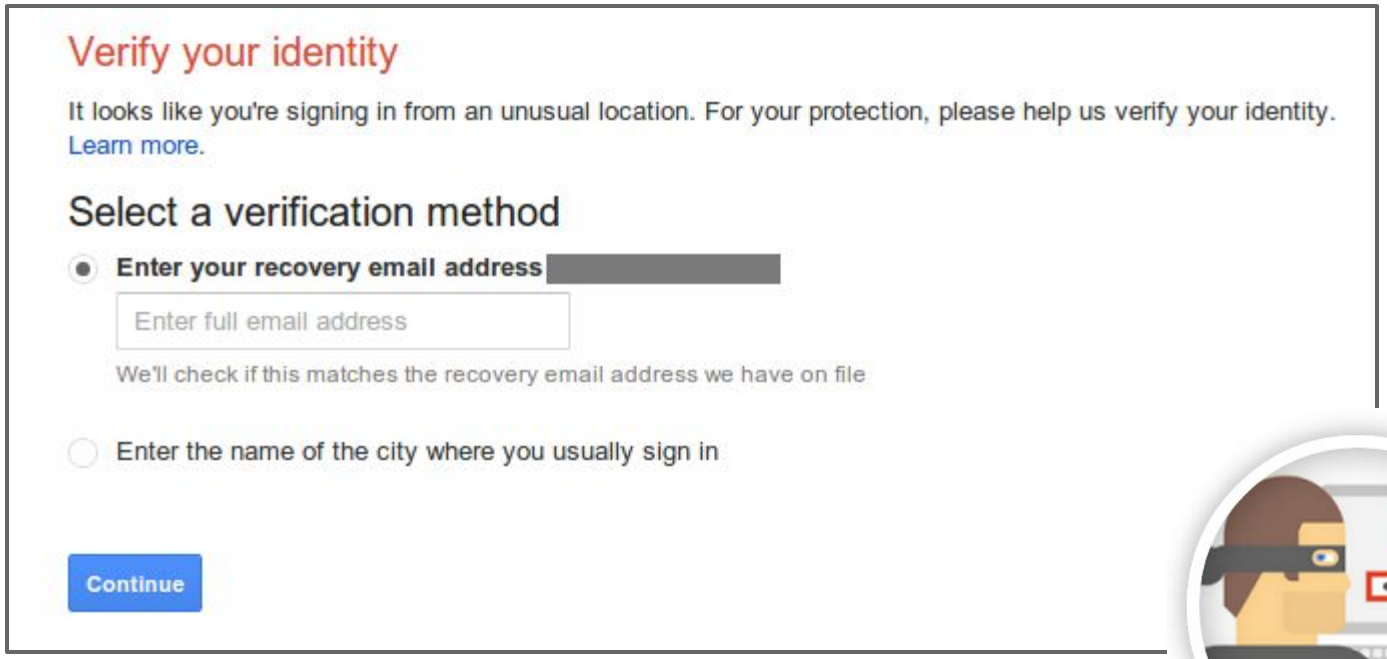
Remission

Manual hijackers mainly use phishing to steal credentials

Type of account phished



Google login challenge



New Google phishing page

Your Google Account is more than just Gmail.

Talk, chat, share, schedule, store, organize, collaborate, discover, and create. Use Google products from Gmail to Google+ to YouTube, view your search history, all with one username and password, all backed up all the time and easy to find at (you guessed it) Google.com.

Take it all with you.

A Google Account lets you access all your stuff — Gmail, photos, and more — from any device. Search by taking pictures, or by voice. Get free turn-by-turn navigation, upload your pictures automatically, and soon even buy things with your phone using Google Wallet.

Enter your username

@gmail.com

Enter your password

Confirm your recovery mobile phone

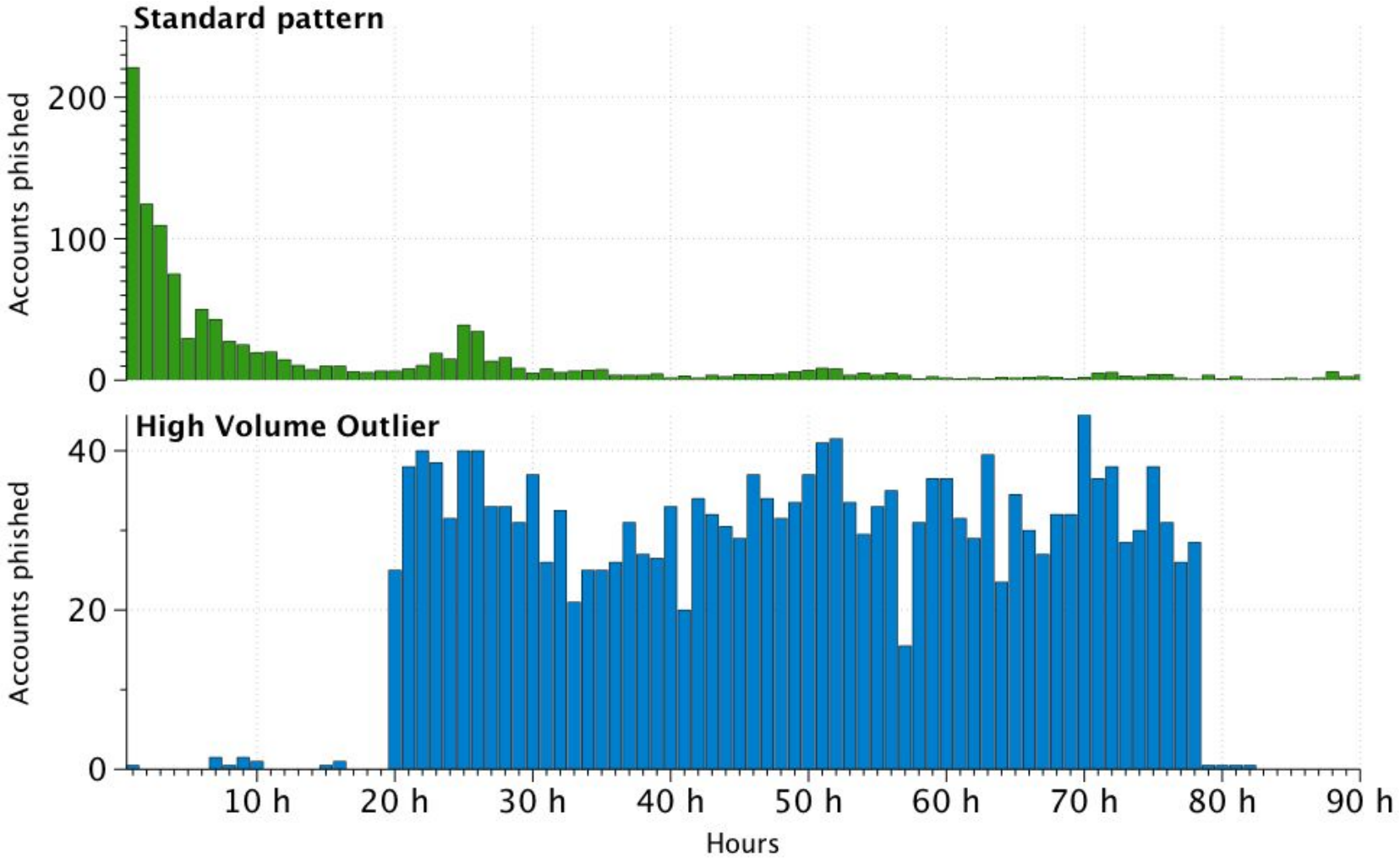
Confirm your recovery email address

Submit

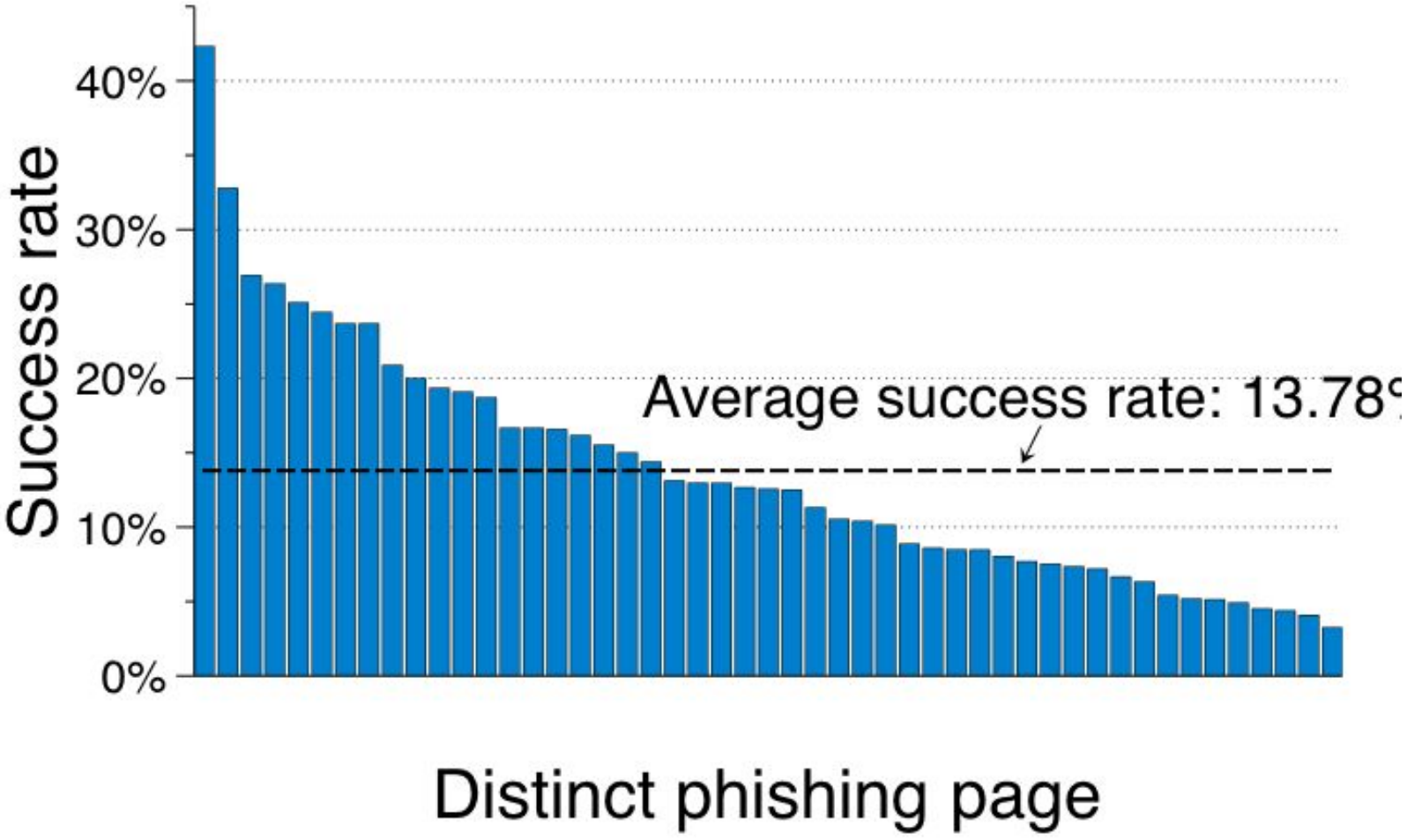
Learn more about why we ask for this information.

Google Drive

Phishing rate

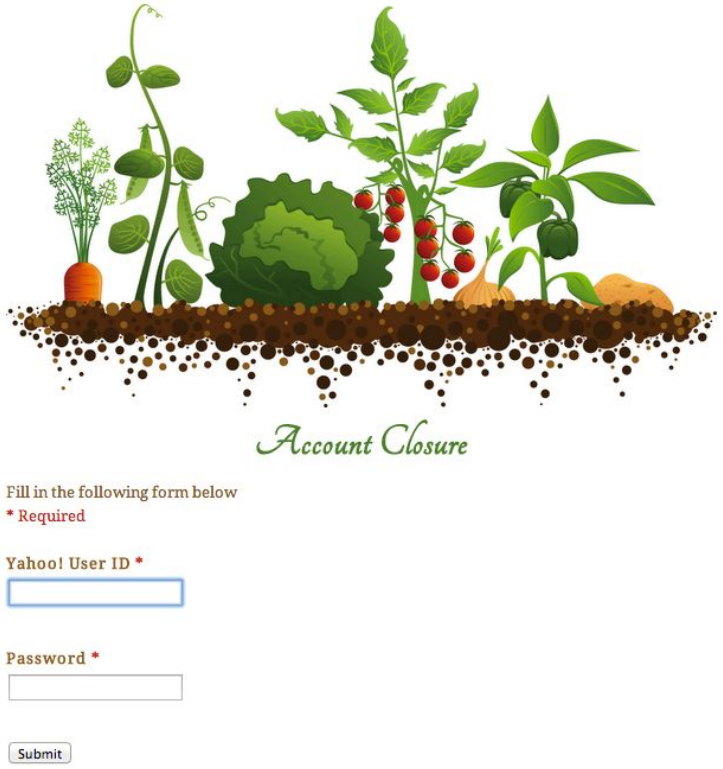


Phishing page efficiency



Phishing page samples

Low success rate page



Unconventional page with high success-rate

Victims are lured to phishing pages via email

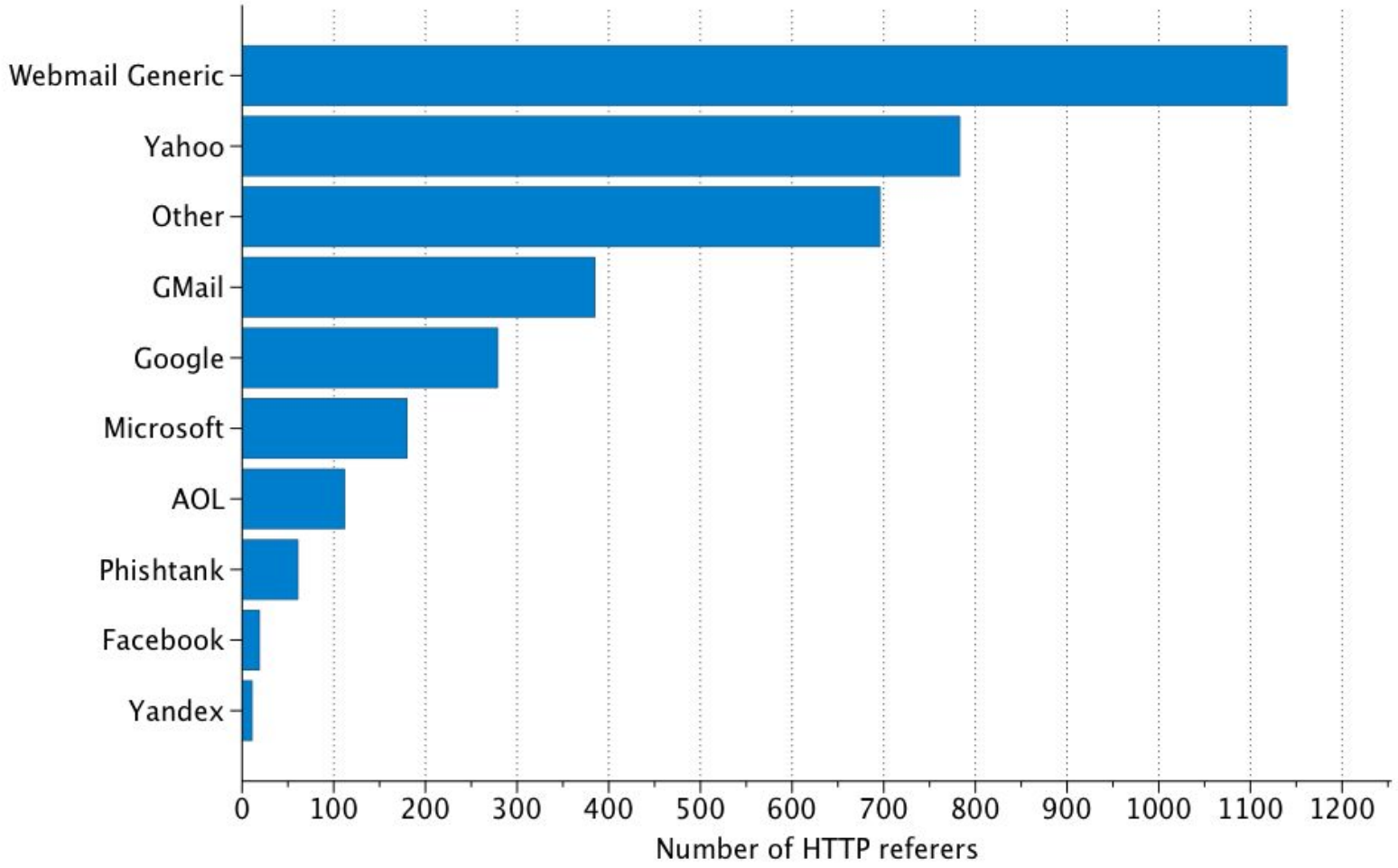
99% of the http requests to phishing page have no refer

Popular webmails (e.g Gmail) and email clients don't set it

Hijacking victims contacts are 36x time more likely to be hijacked in the future

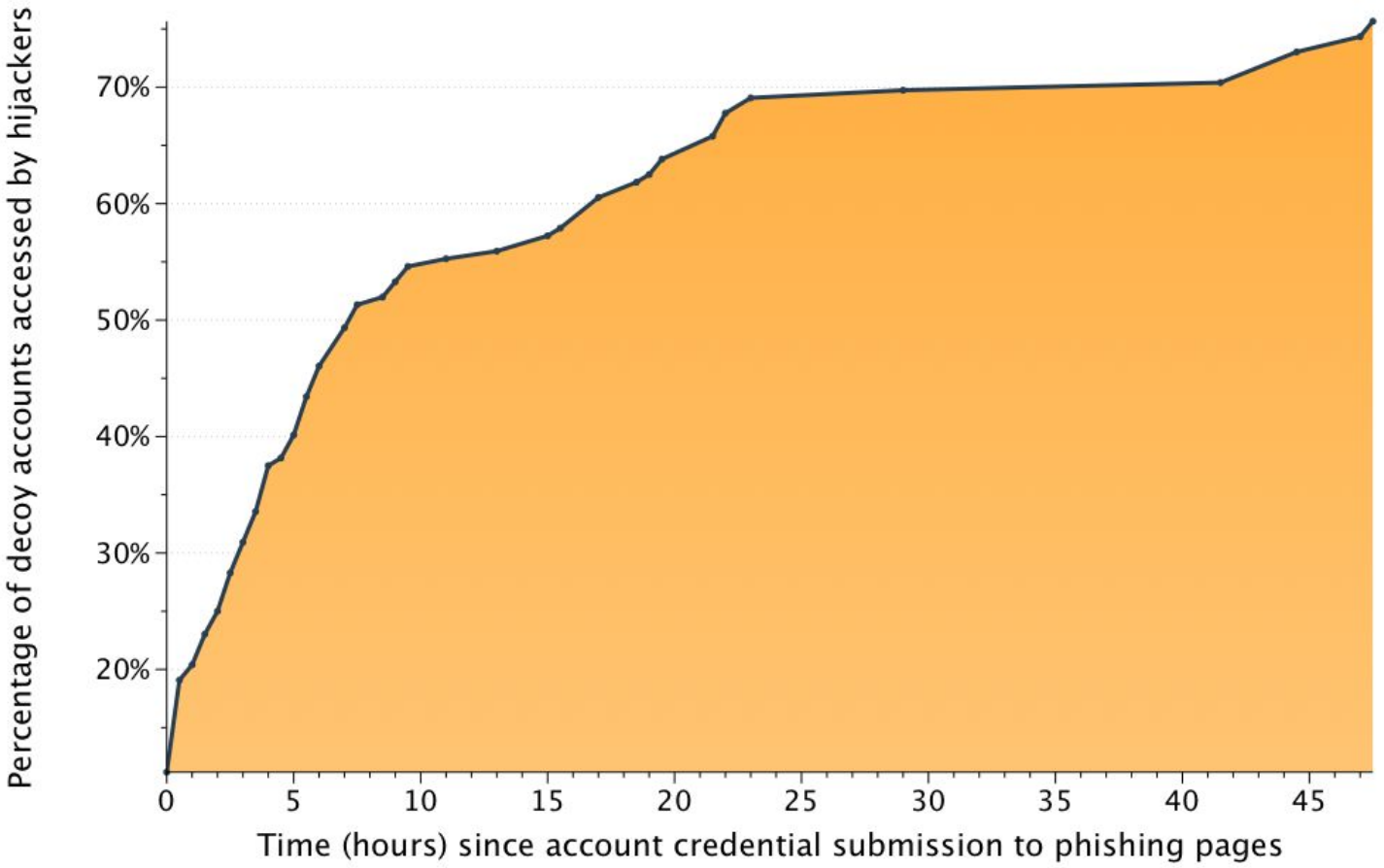
Hijackers abuse victims social circle to find their next victims

HTTP refers breakdown



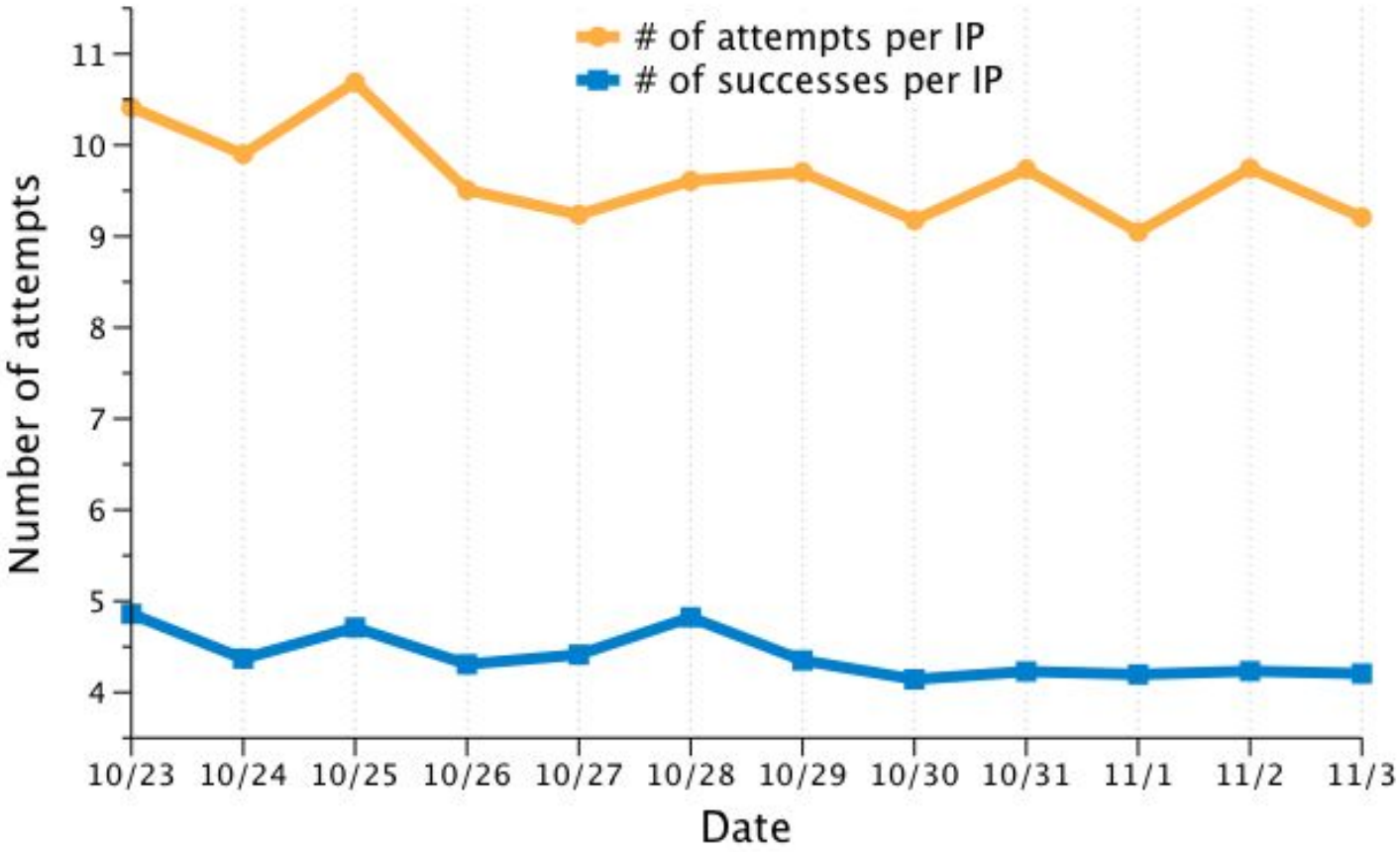
Account exploitation

Time from phishing to compromise



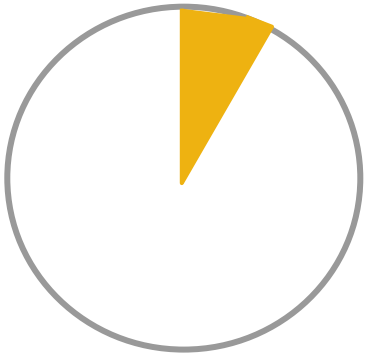
20% of decoy accounts accessed in less than 30 min, 50% within 7h

Hijacking attempt per IPs per day

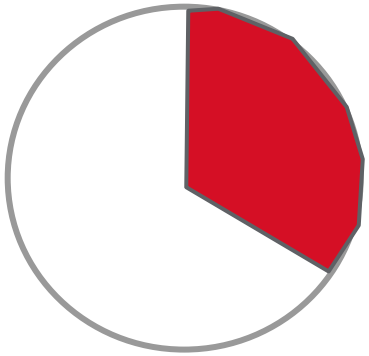


Very few attempts per IPs which make them hard to detect

Time spent per account



Uninteresting account
1 to 3 minutes



Interesting account
15 to 20 minutes

Hijackers only exploit accounts that they deem valuable

Hi xxx,

I'm writing this with **tears in my eyes**, my family and I came down here to **London, England** for a **short vacation** unfortunately **we were mugged** at the park of the hotel where we stayed, all cash, credit card and **cellphones were stolen** off us but luckily for us we still have our passports with us.

We've been to the embassy and the Police here but they're not helping issues at all, Our **return flight leaves in few hours** time from now and am having problems settling my bills.

I was wondering if you can **loan me some money** to pay up the bills and also take a cab to the airport, But any amount you can afford will be appreciated, **I'll refund it to you as soon as I arrive home**.

Write me so I can let you know how to send it.
Thanks,x

Distress to create empathy

Why the victims didn't warn of the trip before hand

Can only be reached via emails

Sense of urgency

Minimizing commitment

Hijackers tactics evolve over time

Locking victims of the account

Change the password (54% → 15%)

Change recovery options (60% → 21%)

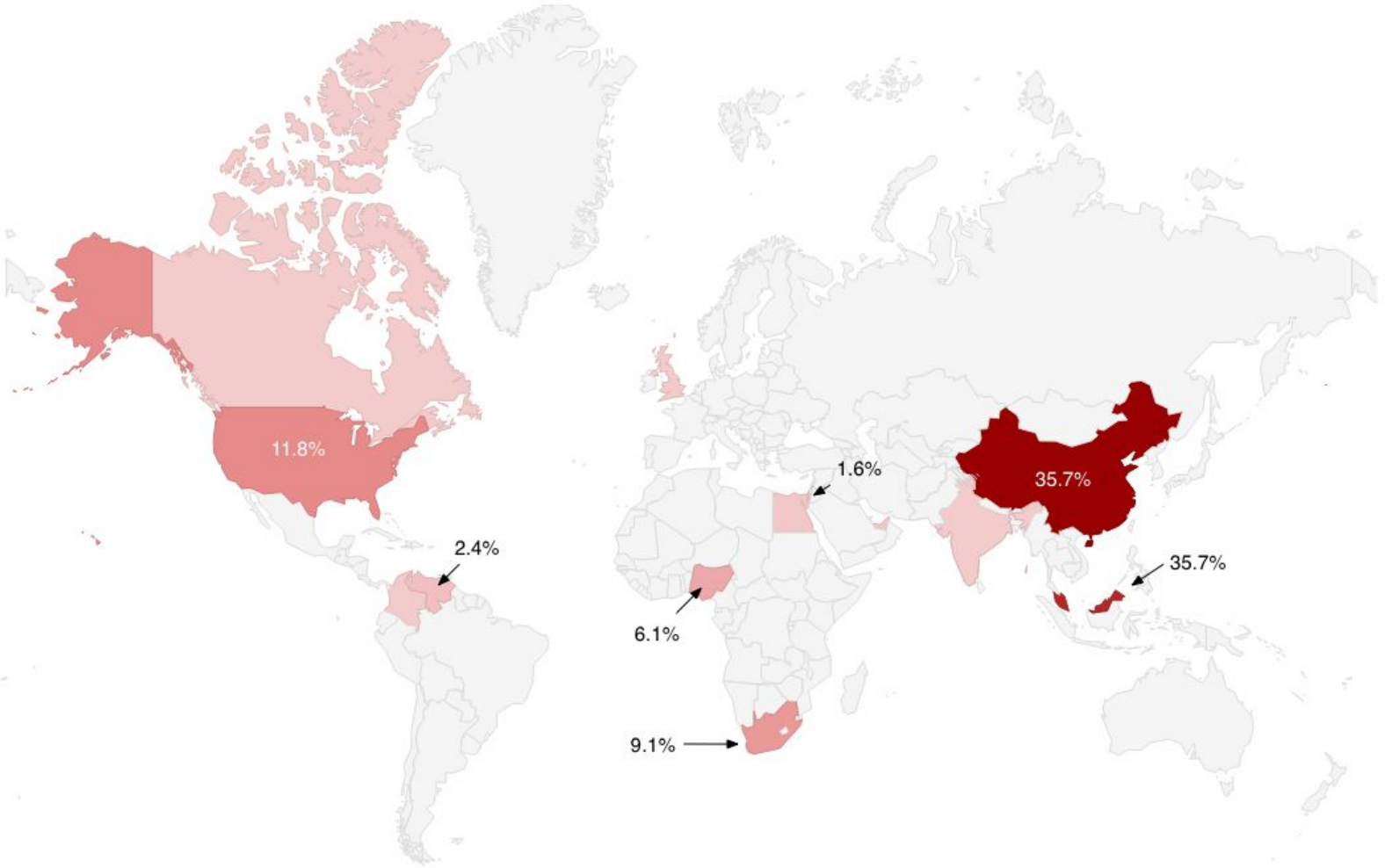
Delete mail (46% → 1.6%)

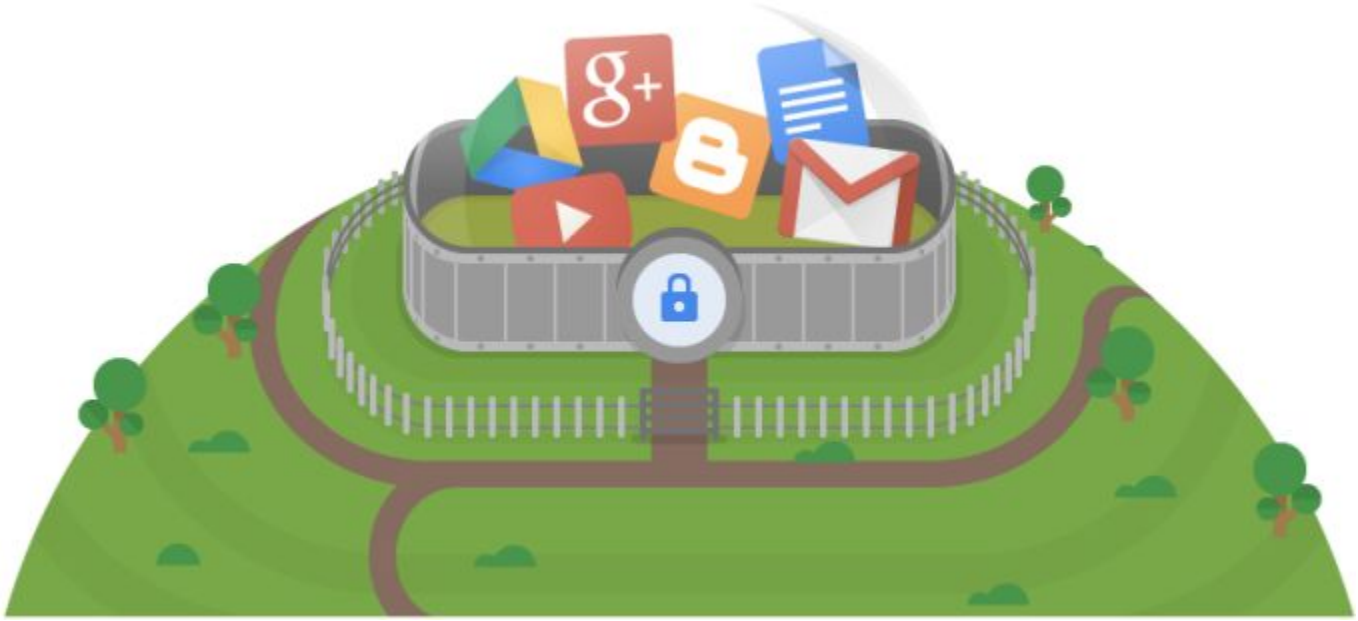
Hiding in the shadow

Reply-to (0? → 26%)

Forwarding rules (0? → 15%)

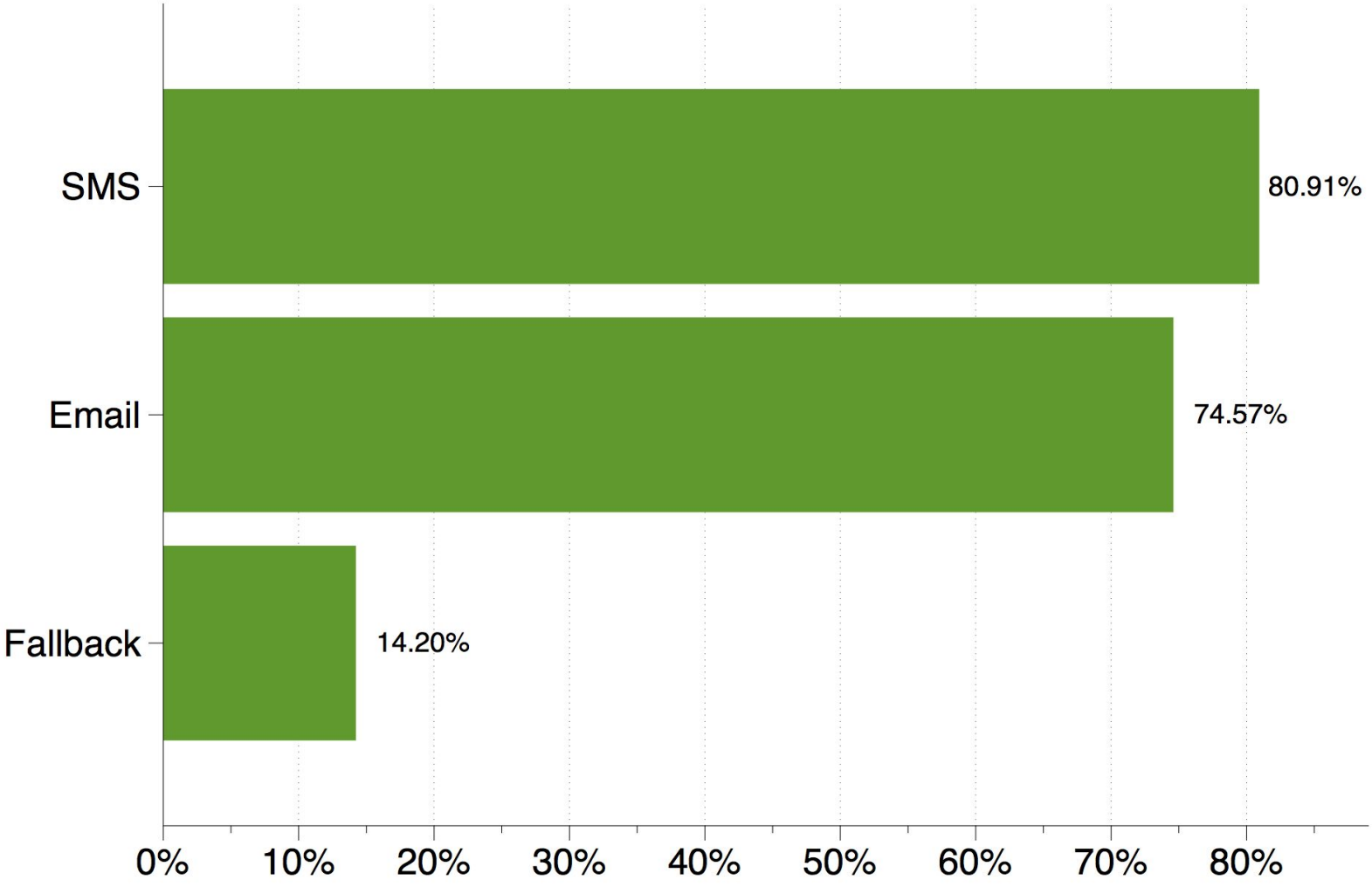
Hijackers origin?





Remediation

Best way to recover accounts: SMS



The perfect defense: second factor

THANKS!

elieb@google.com

Questions?