KnowBe4
Human error. Conquered.

Many Ways to Hack Multifactor Authentication

Roger Grimes
Data-Driven Defense Evangelist,
KnowBe4, Inc.
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

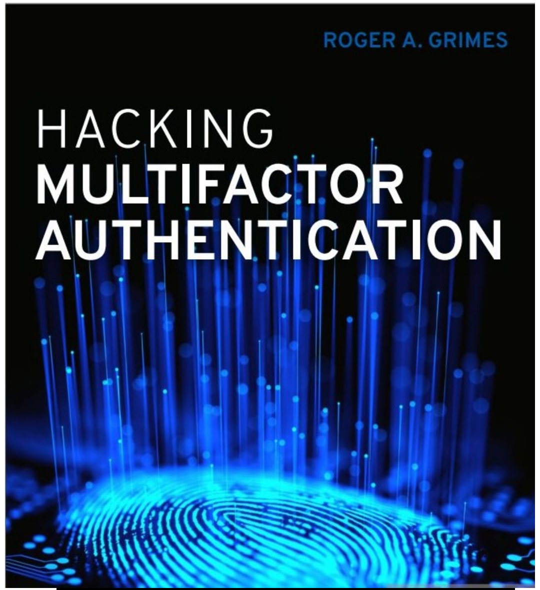
About Roger

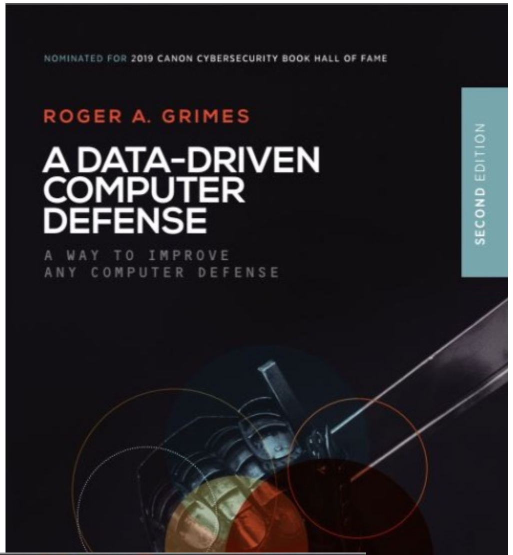
- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,200 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certification exams passed include:

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

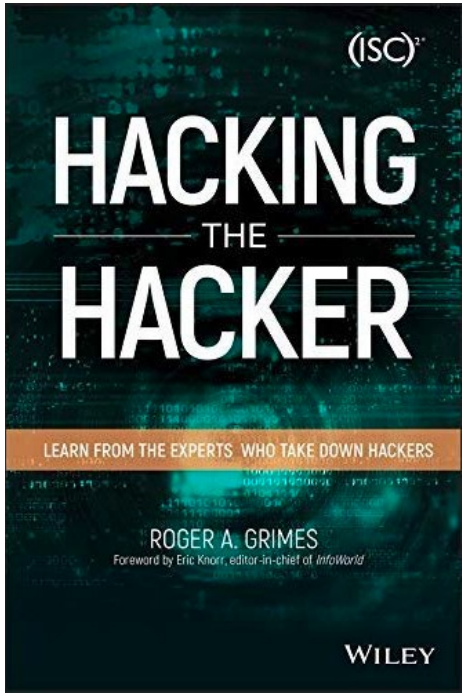
Roger's Books

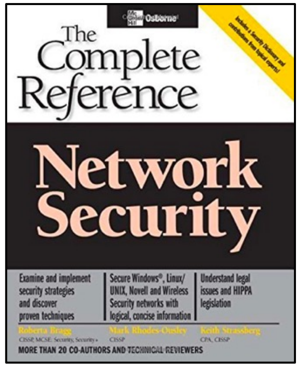


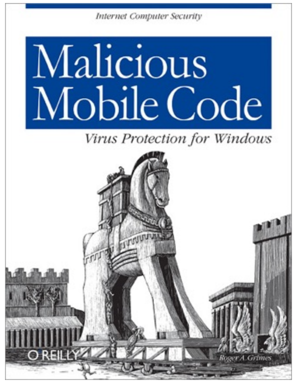


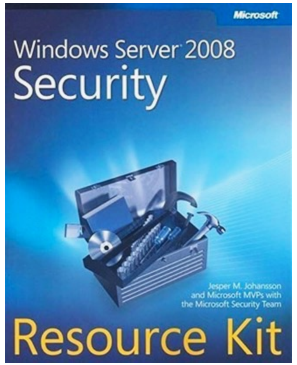
RSA
June 2018
Recommended
Book of the
Month

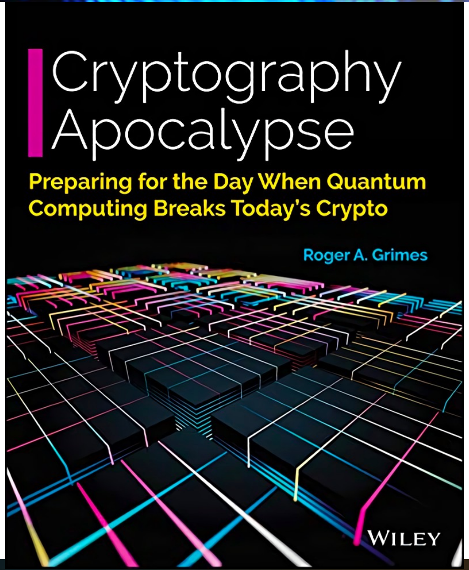
Postgraduate School


(ISC)²
HACKING
THE
HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

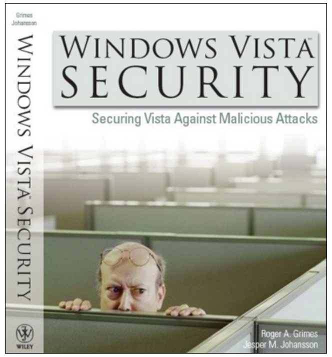

Osborne
Includes a Security Dictionary and contributions from topical experts!
The
Complete
Reference
Network
Security
Examine and implement security strategies and discover proven techniques
Secure Windows®, Linux/UNIX, Novell and Wireless Security networks with logical, concise information
Understand legal issues and HIPPA legislation
Roberta Bragg
CISSP, MCSE: Security, Security+
Mark Rhodes-Ousley
CISSP
Keith Strassberg
CPA, CISSP
MORE THAN 20 CO-AUTHORS AND TECHNICAL REVIEWERS

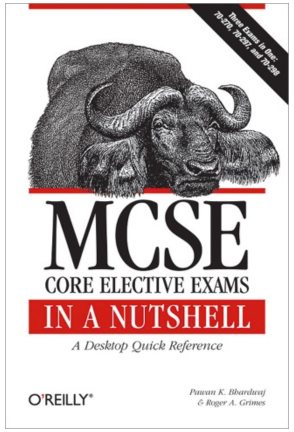


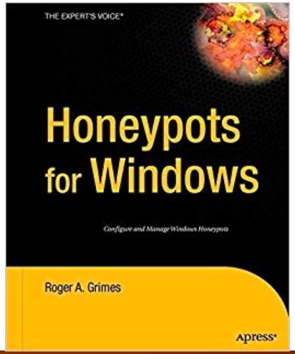



Cryptography
Apocalypse
Preparing for the Day When Quantum
Computing Breaks Today's Crypto
Roger A. Grimes
WILEY

Programmer to Programmer™
Professional
Windows
Desktop and Server
Hardening
Roger A. Grimes
wrox
Updates, downloads, and Wrox technical support at www.wrox.com







About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER®

WAVE LEADER 2022

Security Awareness And Training Solutions

TRAIN

PHISH

ANALYZE

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES

Inc. 500

Gartner peerinsights customers' choice 2021 ™

Today's Presentation

- Multifactor Authentication Intro
- Hacking MFA
- Lessons and Recommendations

Multifactor Authentication Intro

Introduction to Multifactor Authentication

Factors

- Something You Know
  - Password, PIN, Connect the Dots, etc.
- Something You Have
  - USB token, smartcard, RFID transmitter, dongle, etc.
- Something You Are
  - Biometrics, fingerprints, retina scan, smell
- Contextual, behavioral analytics, actions, location, etc.

Introduction to Multifactor Authentication

Factors

- Single Factor
- Two Factor (2FA)
- Multifactor (MFA)
  - 2-3 or more factors

- Two or more of the same factor isn't as strong as different types of factors

Introduction to Multifactor Authentication

Use MFA

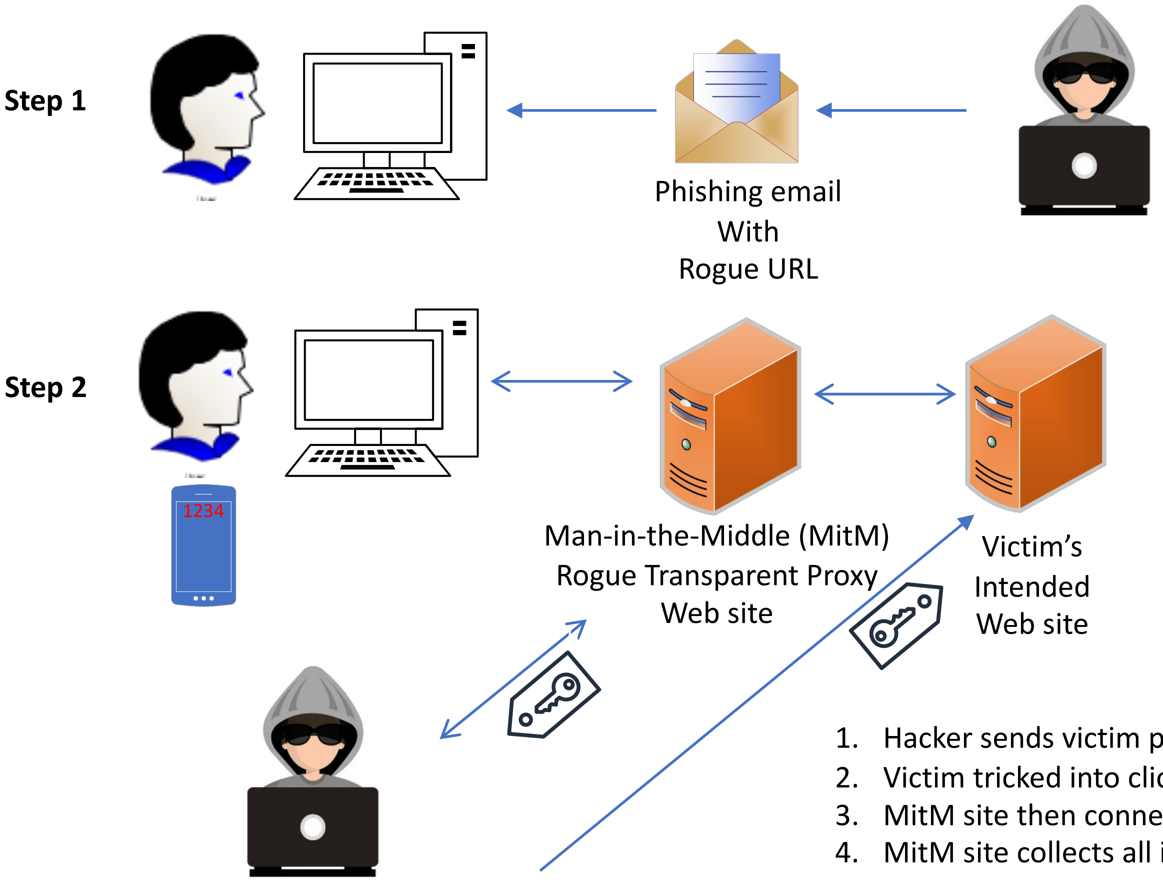
- All things considered, MFA is usually better than 1FA
- We all should strive to use phishing-resistant MFA wherever it makes sense and then whenever possible
- But MFA isn’t unhackable

Hacking MFA

MFA Bypass Hack

Network Session Hijacking

Network Session Hijacking Proxy Theft Logical Diagram

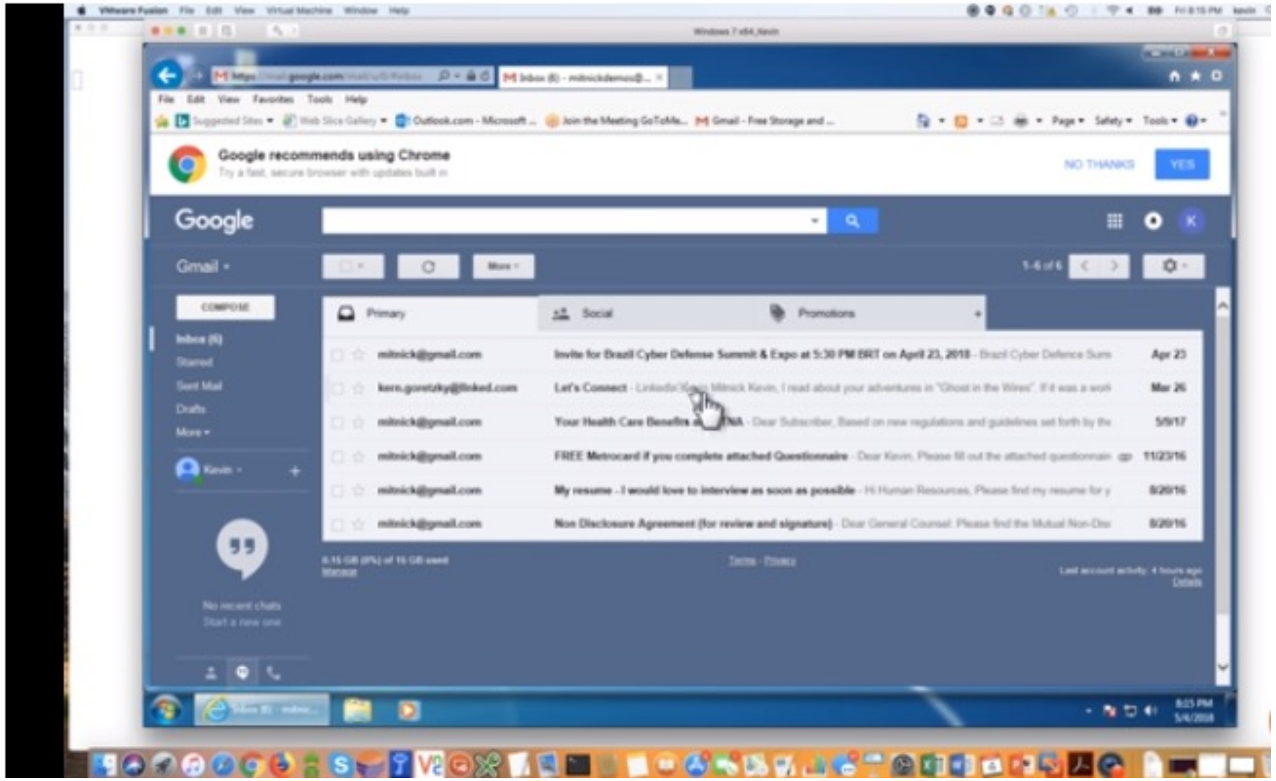


1. Hacker sends victim phishing email with rogue URL
2. Victim tricked into clicking on rogue URL, taking victim to rogue MitM site
3. MitM site then connects to victim's intended legitimate, real, web site
4. MitM site collects all info/data sent between victim and real web site; and vice-versa
5. Hacker can steal victim's logon creds, MFA, access control token cookie, etc.
6. Hacker uses victim's access control token cookie to logon

MFA Hacks

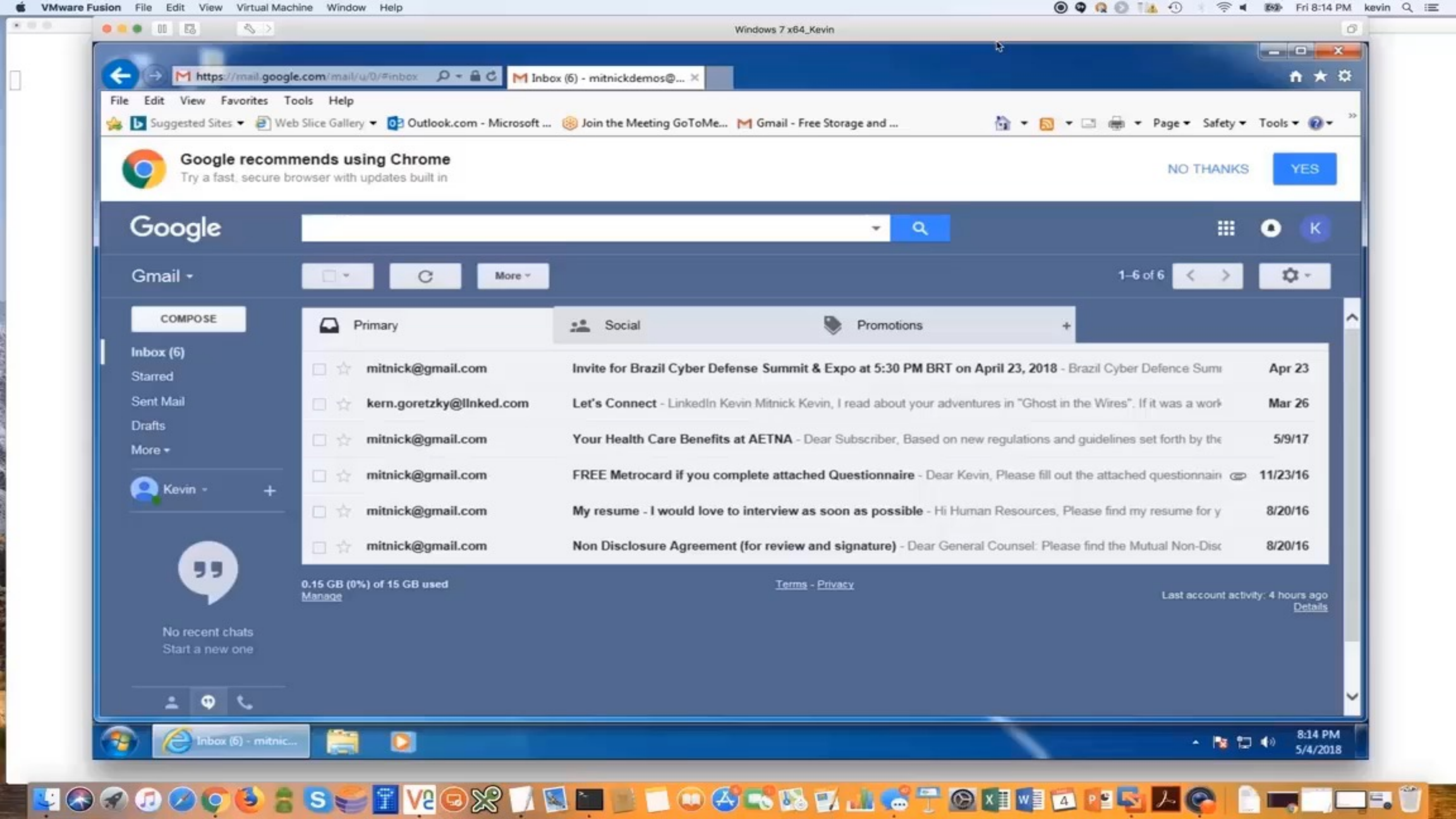
Network Session Hijacking

Kevin Mitnick Hack Demo



mitnick@gmail.com	Invite for Brazil Cyber Defense Summit & Expo at 5:30 PM BRT on April 23, 2018 - Brazil Cyber Defence Sum	Apr 23
kern.goretzky@linked.com	Let's Connect - LinkedIn Kevin Mitnick Kevin, I read about your adventures in "Ghost in the Wires". If it was a work	Mar 26
mitnick@gmail.com	Your Health Care Benefits at CNA - Dear Subscriber, Based on new regulations and guidelines set forth by the	5/9/17
mitnick@gmail.com	FREE Metrocard if you complete attached Questionnaire - Dear Kevin, Please fill out the attached questionnair	11/23/16
mitnick@gmail.com	My resume - I would love to interview as soon as possible - Hi Human Resources, Please find my resume for y	8/20/16
mitnick@gmail.com	Non Disclosure Agreement (for review and signature) - Dear General Counsel: Please find the Mutual Non-Dis	8/20/16

https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedin-2-factor-auth.-see-this-kevin-mitnick-video



Google recommends using Chrome
Try a fast, secure browser with updates built in

NO THANKS YES

mitnick@gmail.com	**Invite for Brazil Cyber Defense Summit & Expo at 5:30 PM BRT on April 23, 2018** - Brazil Cyber Defence Sumi	Apr 23
kern.goretzky@llnked.com	**Let's Connect** - LinkedIn Kevin Mitnick Kevin, I read about your adventures in "Ghost in the Wires". If it was a work	Mar 26
mitnick@gmail.com	**Your Health Care Benefits at AETNA** - Dear Subscriber, Based on new regulations and guidelines set forth by the	5/9/17
mitnick@gmail.com	**FREE Metrocard if you complete attached Questionnaire** - Dear Kevin, Please fill out the attached questionnair	11/23/16
mitnick@gmail.com	**My resume - I would love to interview as soon as possible** - Hi Human Resources, Please find my resume for y	8/20/16
mitnick@gmail.com	**Non Disclosure Agreement (for review and signature)** - Dear General Counsel: Please find the Mutual Non-Disc	8/20/16

0.15 GB (0%) of 15 GB used
Manage

Terms - Privacy

Last account activity: 4 hours ago
Details

MFA Hacks

Network Session Hijacking

Kevin Mitnick Hack Demo

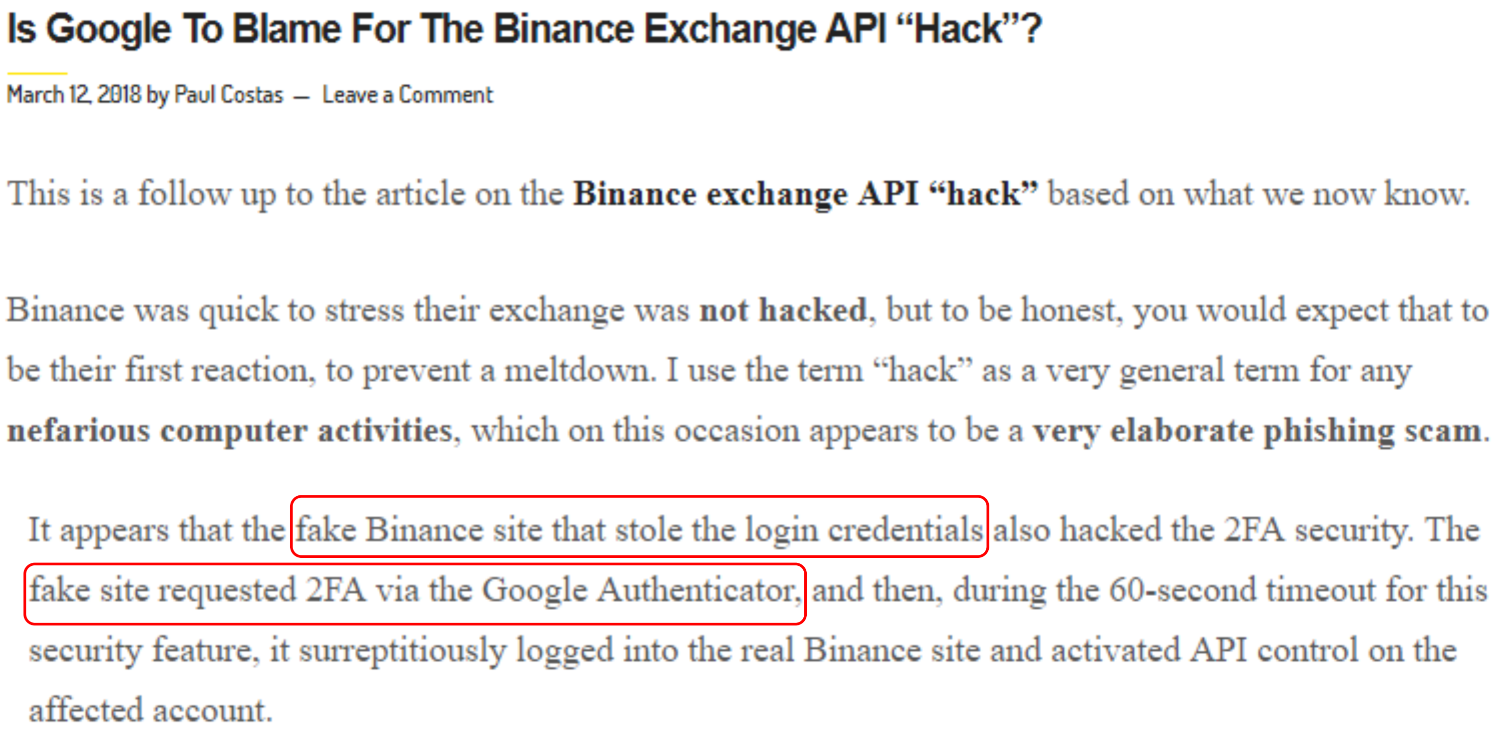
1. Phishing email contained URL to fake look-alike/sound-alike web site that was really an evil proxy
2. Email tricked user into visiting evil proxy web site
3. User typed in credentials, which proxy, now pretending to be the legitimate customer, presented to legitimate web site
4. Legitimate web site sent back legitimate session token, which Kevin then stole and replayed to take over user's session

- Kevin used Evilginx (https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/)
- One example hack out of the dozens, if not hundreds of ways to do session hijacking, even if MFA is involved

MFA Hacks

Network Session Hijacking

Real-World Example



Is Google To Blame For The Binance Exchange API "Hack"?

March 12, 2018 by Paul Costas — Leave a Comment

This is a follow up to the article on the **Binance exchange API "hack"** based on what we now know.

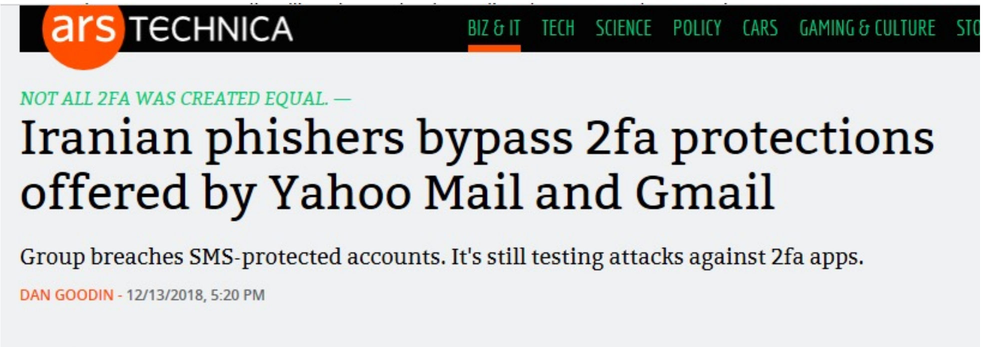
Binance was quick to stress their exchange was **not hacked**, but to be honest, you would expect that to be their first reaction, to prevent a meltdown. I use the term "hack" as a very general term for any **nefarious computer activities**, which on this occasion appears to be a **very elaborate phishing scam**.

It appears that the fake Binance site that stole the login credentials also hacked the 2FA security. The fake site requested 2FA via the Google Authenticator, and then, during the 60-second timeout for this security feature, it surreptitiously logged into the real Binance site and activated API control on the affected account.

MFA Hacks

Network Session Hijacking

Real-World Example



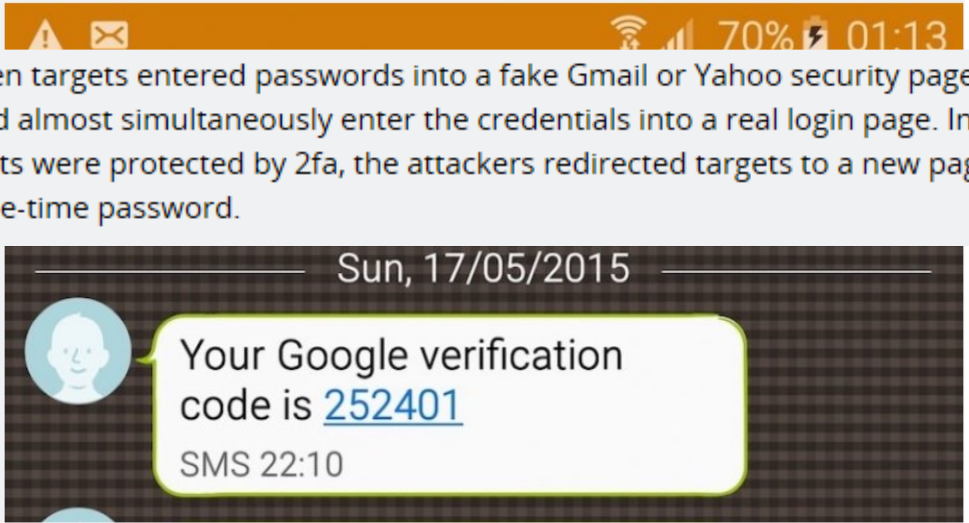
NOT ALL 2FA WAS CREATED EQUAL —

Iranian phishers bypass 2fa protections offered by Yahoo Mail and Gmail

Group breaches SMS-protected accounts. It's still testing attacks against 2fa apps.

DAN GOODIN - 12/13/2018, 5:20 PM

messages. When targets entered passwords into a fake Gmail or Yahoo security page, the attackers would almost simultaneously enter the credentials into a real login page. In the event targets' accounts were protected by 2fa, the attackers redirected targets to a new page that requested a one-time password.



Sun, 17/05/2015

Your Google verification code is 252401

SMS 22:10

https://arstechnica.com/information-technology/2018/12/iranian-phishers-bypass-2fa-protections-offered-by-yahoo-mail-and-gmail/

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

If endpoint gets compromised, MFA isn’t going to help you

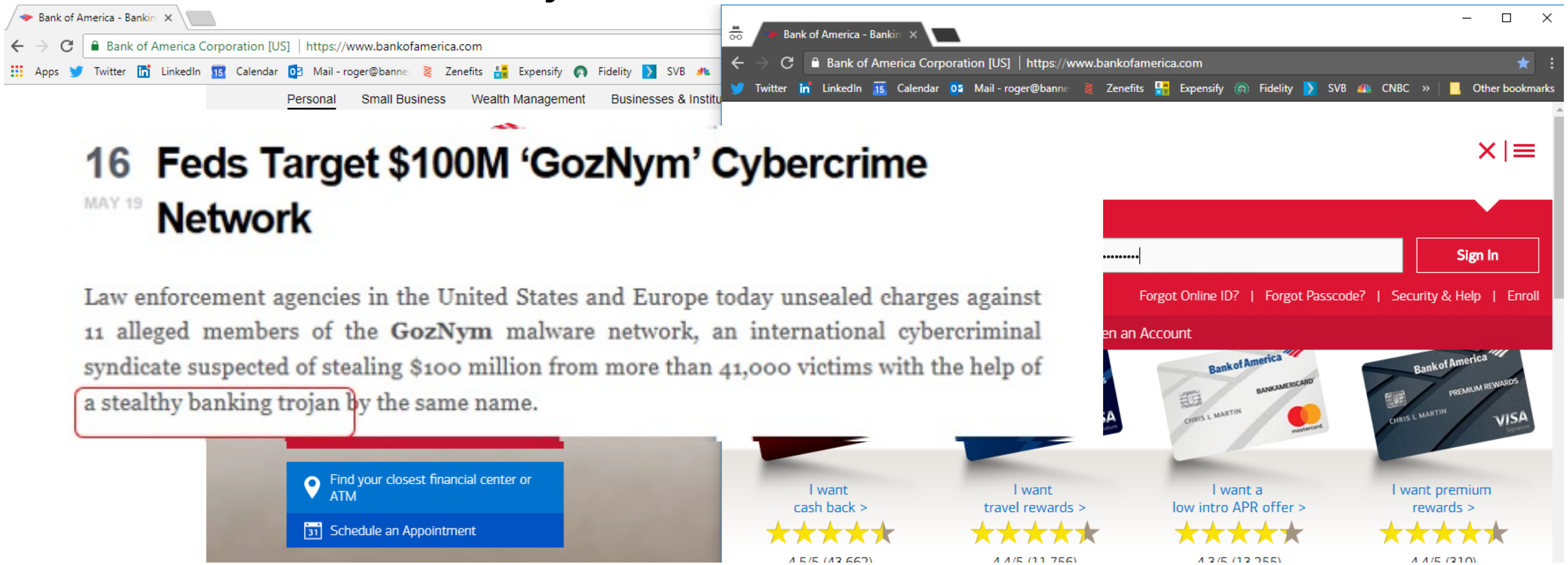
- Attacker can just do everything they want that the user is allowed to do after successful authentication
- Start a second hidden browser session
- Directly steal session cookies
- Insert backdoors
- Invalidate protection all together

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

- Start up a second session that the user isn’t even aware
  - Ex. Bancos trojans



16 MAY 19

Feds Target $100M ‘GozNym’ Cybercrime Network

Law enforcement agencies in the United States and Europe today unsealed charges against 11 alleged members of the **GozNym** malware network, an international cybercriminal syndicate suspected of stealing $100 million from more than 41,000 victims with the help of a stealthy banking trojan by the same name.

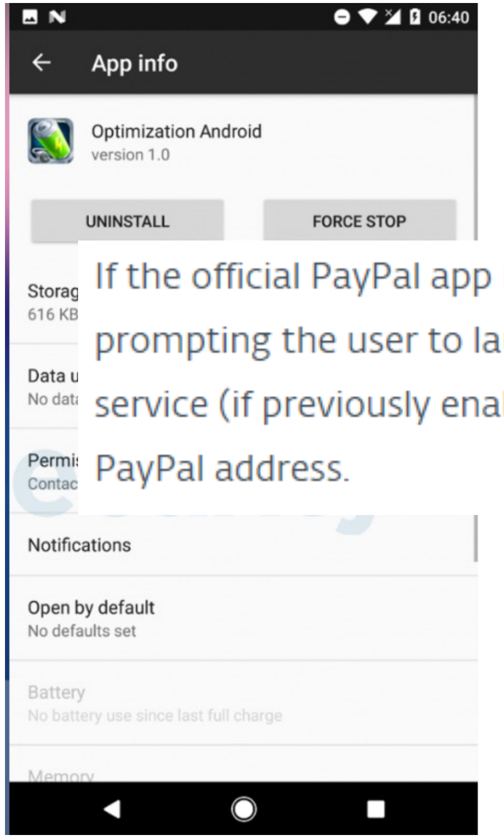
Bank of America - Bankin
Bank of America Corporation [US] | https://www.bankofamerica.com
Personal
Small Business
Wealth Management
Businesses & Institu
Find your closest financial center or ATM
Schedule an Appointment
Sign In
Forgot Online ID? | Forgot Passcode? | Security & Help | Enroll
en an Account
I want cash back >
I want travel rewards >
I want a low intro APR offer >
I want premium rewards >

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

- Start up a second session that the user isn't even aware



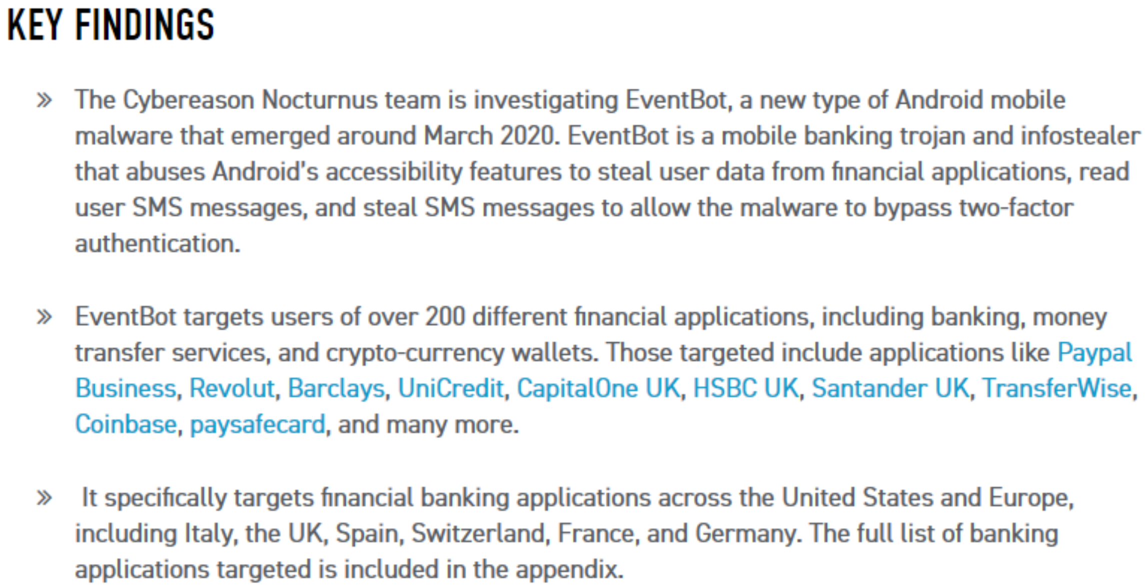
If the official PayPal app is installed on the compromised device, the malware displays a notification alert prompting the user to launch it. Once the user opens the PayPal app and logs in, the malicious accessibility service (if previously enabled by the user) steps in and mimics the user's clicks to send money to the attacker's PayPal address.

https://www.youtube.com/watch?v=yn04eLoivX8

MFA Hacks

Endpoint Attacks

https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born



KEY FINDINGS

» The Cybereason Nocturnus team is investigating EventBot, a new type of Android mobile malware that emerged around March 2020. EventBot is a mobile banking trojan and infostealer that abuses Android's accessibility features to steal user data from financial applications, read user SMS messages, and steal SMS messages to allow the malware to bypass two-factor authentication.

» EventBot targets users of over 200 different financial applications, including banking, money transfer services, and crypto-currency wallets. Those targeted include applications like Paypal Business, Revolut, Barclays, UniCredit, CapitalOne UK, HSBC UK, Santander UK, TransferWise, Coinbase, paysafecard, and many more.

» It specifically targets financial banking applications across the United States and Europe, including Italy, the UK, Spain, Switzerland, France, and Germany. The full list of banking applications targeted is included in the appendix.

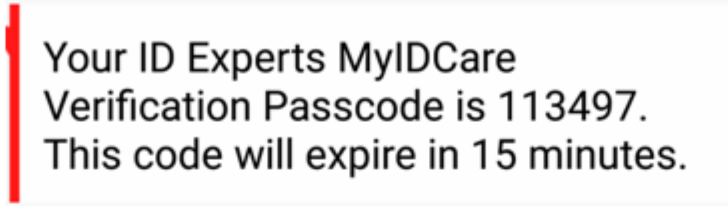
Security researchers have warned that newly created mobile banking malware can not only grab passwords for more than 200 financial apps, but intercept two-factor authentication codes as well.

Posing as legitimate applications such as a Flash update, installed from unauthorised or compromised sources, EventBot relies upon the unsuspecting user granting it a bunch of permissions from reading external storage and SMS to creating system alert windows that can be shown on top of other apps.

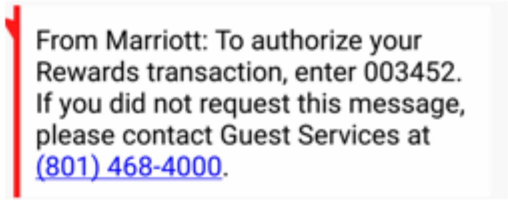
MFA Hacks

SMS-based MFA

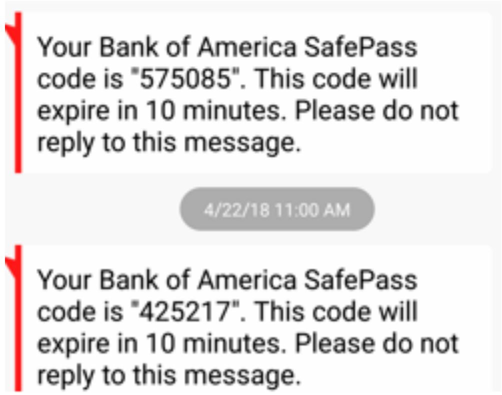
- Many MFA methods included sending additional authentication code via a user’s cell phone short message service (SMS)



Your ID Experts MyIDCare Verification Passcode is 113497. This code will expire in 15 minutes.



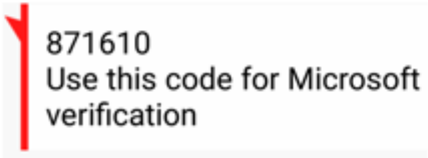
From Marriott: To authorize your Rewards transaction, enter 003452. If you did not request this message, please contact Guest Services at (801) 468-4000.



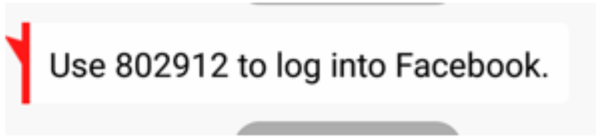
Your Bank of America SafePass code is "575085". This code will expire in 10 minutes. Please do not reply to this message.

4/22/18 11:00 AM

Your Bank of America SafePass code is "425217". This code will expire in 10 minutes. Please do not reply to this message.



871610
Use this code for Microsoft verification



Use 802912 to log into Facebook.

MFA Hacks

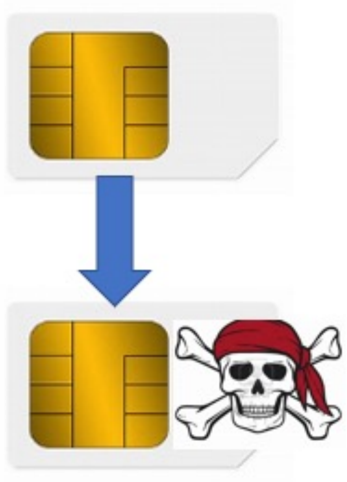
SIM Swapping

SIM Basics

- SIM stands for **S**ubscriber **I**dentity **M**odule
- SIM storage contains the cell phone vendors network's information, device ID, and the subscriber's (user/owner) phone number and other info, plus can store app data
- Traditionally was stored on micro-SD card
- Today, often stored and moved digitally
- An activated phone with your SIM info will act as your phone, accept and receive phone calls and SMS messages

MFA Hacks

SIM Swapping Attacks

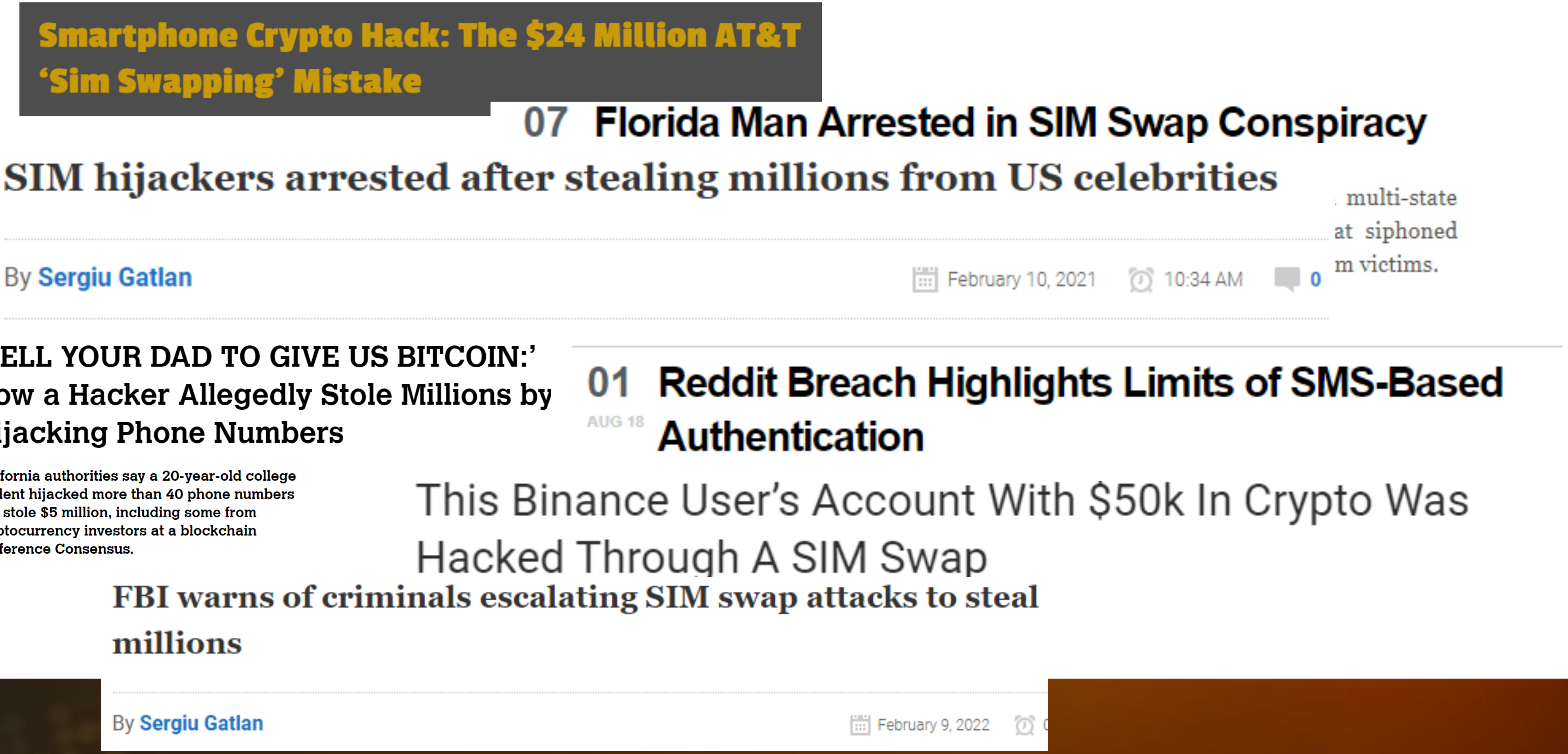


- In a SIM swapping attack, the attacker transfers the victim’s SIM information to another phone, allowing the attacker to get the any sent codes used by SMS-based MFA solutions
    - Old phone “silently” stops working
- Usually done by hack social engineering cell phone vendor’s support techs; or using a compromised insider
- Often is done using cell phone network logon information the attacker has previously phished out of the victim using another precursor phishing attack
- Some mobile phone trojans steal SIM information
- NIST (in SP 800-63) does not accept SMS codes as valid authentication because of how easy it is to hack

MFA Hacks

SIM Swapping Attacks

- Has been successfully used in many of the world's biggest personal attacks



Smartphone Crypto Hack: The $24 Million AT&T 'Sim Swapping' Mistake

07 **Florida Man Arrested in SIM Swap Conspiracy**

SIM hijackers arrested after stealing millions from US celebrities

By Sergiu Gatlan February 10, 2021 10:34 AM 0

multi-state
at siphoned
m victims.

'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers

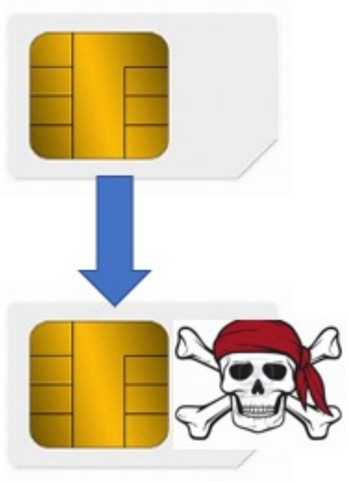
California authorities say a 20-year-old college student hijacked more than 40 phone numbers and stole $5 million, including some from cryptocurrency investors at a blockchain conference Consensus.

01 AUG 18 **Reddit Breach Highlights Limits of SMS-Based Authentication**

This Binance User's Account With $50k In Crypto Was Hacked Through A SIM Swap

FBI warns of criminals escalating SIM swap attacks to steal millions

By Sergiu Gatlan February 9, 2022



For $16 I Can Get Your SMS Messages Sent to Me

SIM Reroute Attacks

- Not a SIM swap attack
- Legit companies allow SMS messages to be re-routed
- Requires “Letter of Authorization”
  - Supposed to have a legit reason for the re-route
  - Must confirm you aren’t doing anything illegal
- Not every rerouting service verifies legitimacy of request
- https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery Hack

- There is an inherent problem in that SMS message origination cannot be easily authenticated within SMS itself
- Anyone can claim to be anyone

To pull off hacker must have:

- You email address and associated phone number

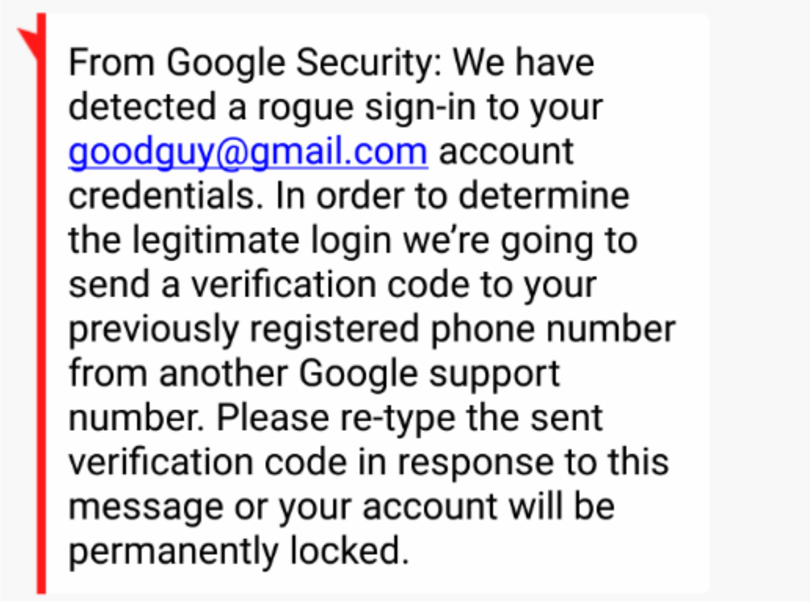
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

1. Hacker sends you a text pretending to be from your email provider asking for your forthcoming SMS PIN reset code



From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

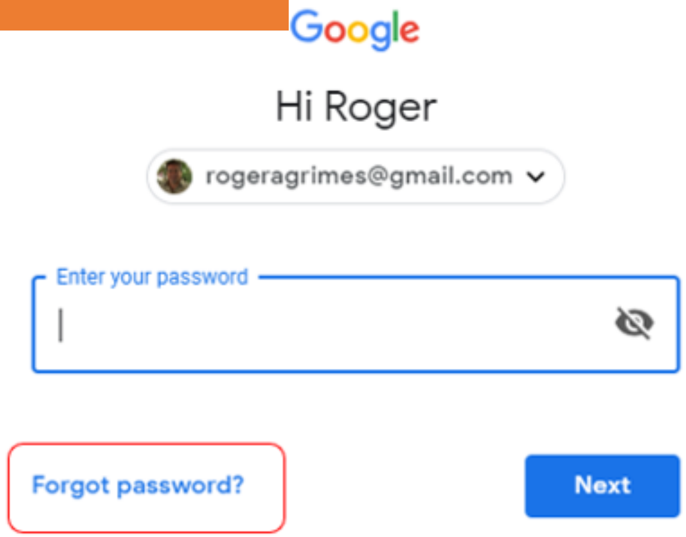
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

2. Hacker forces your email account into SMS PIN recovery



Google

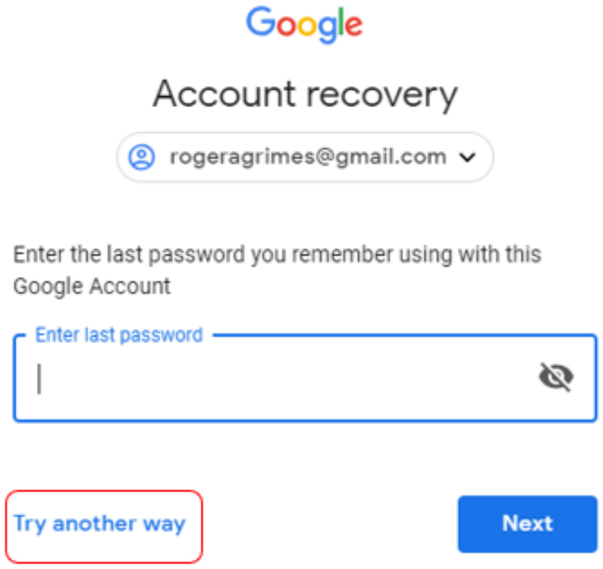
Hi Roger

rogeragrimes@gmail.com

Enter your password

Forgot password?

Next



Google

Account recovery

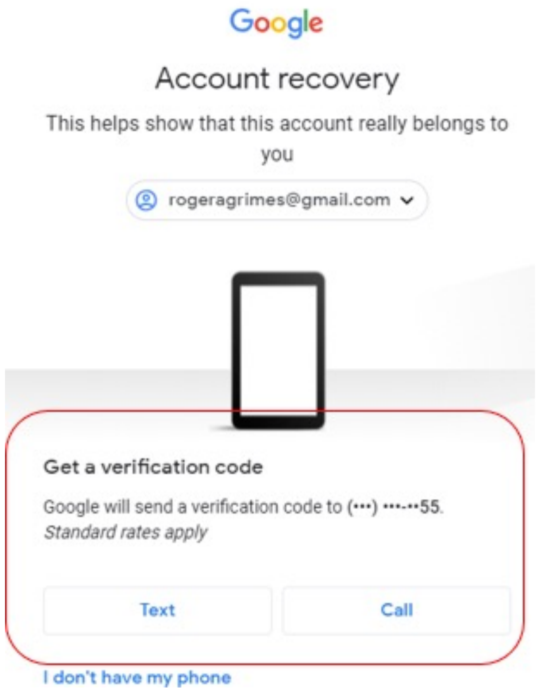
rogeragrimes@gmail.com

Enter the last password you remember using with this Google Account

Enter last password

Try another way

Next



Google

Account recovery

This helps show that this account really belongs to you

rogeragrimes@gmail.com

Get a verification code

Google will send a verification code to (•••) •••-••55.
Standard rates apply

Text

Call

I don't have my phone

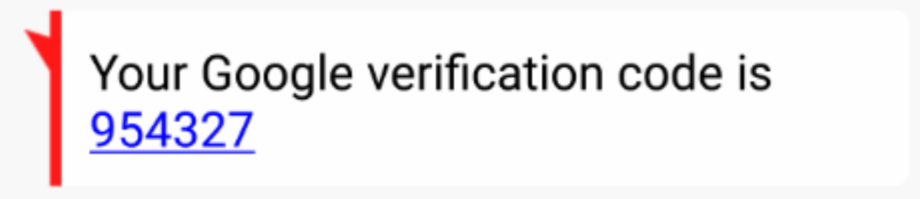
Rogue Recoveries

SMS Rogue Recovery

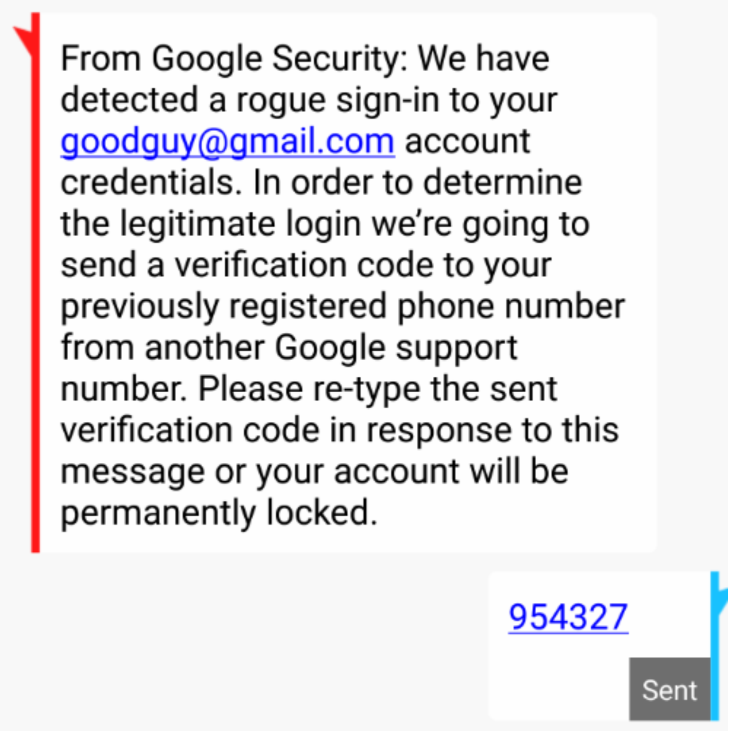
Hacking Into Your Email Using Recovery Methods

Steps

3. You get text from vendor with your reset code, which you then send to other number



Your Google verification code is 954327



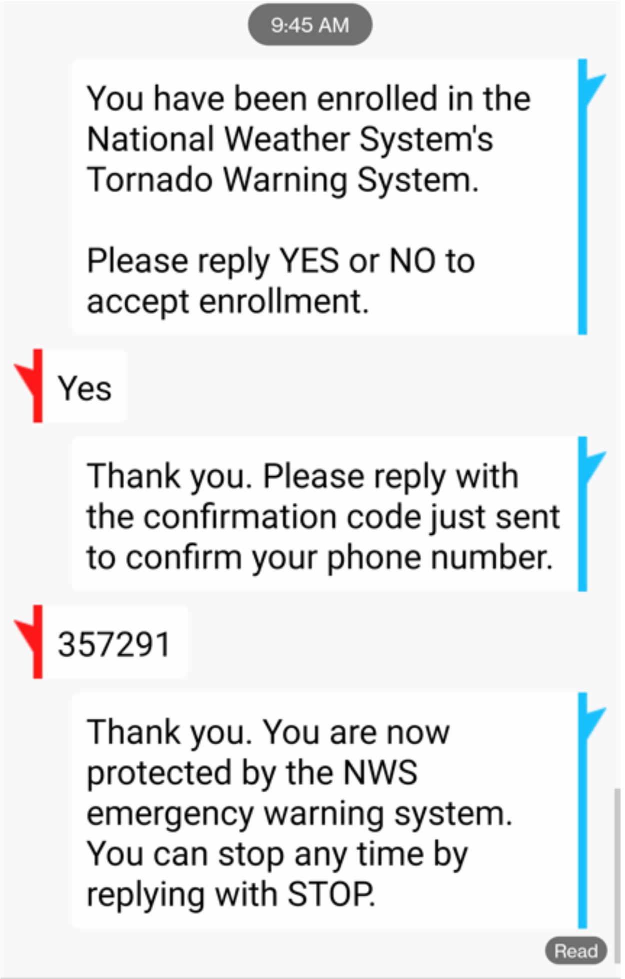
From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

954327

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery



9:45 AM

You have been enrolled in the National Weather System's Tornado Warning System.

Please reply YES or NO to accept enrollment.

Yes

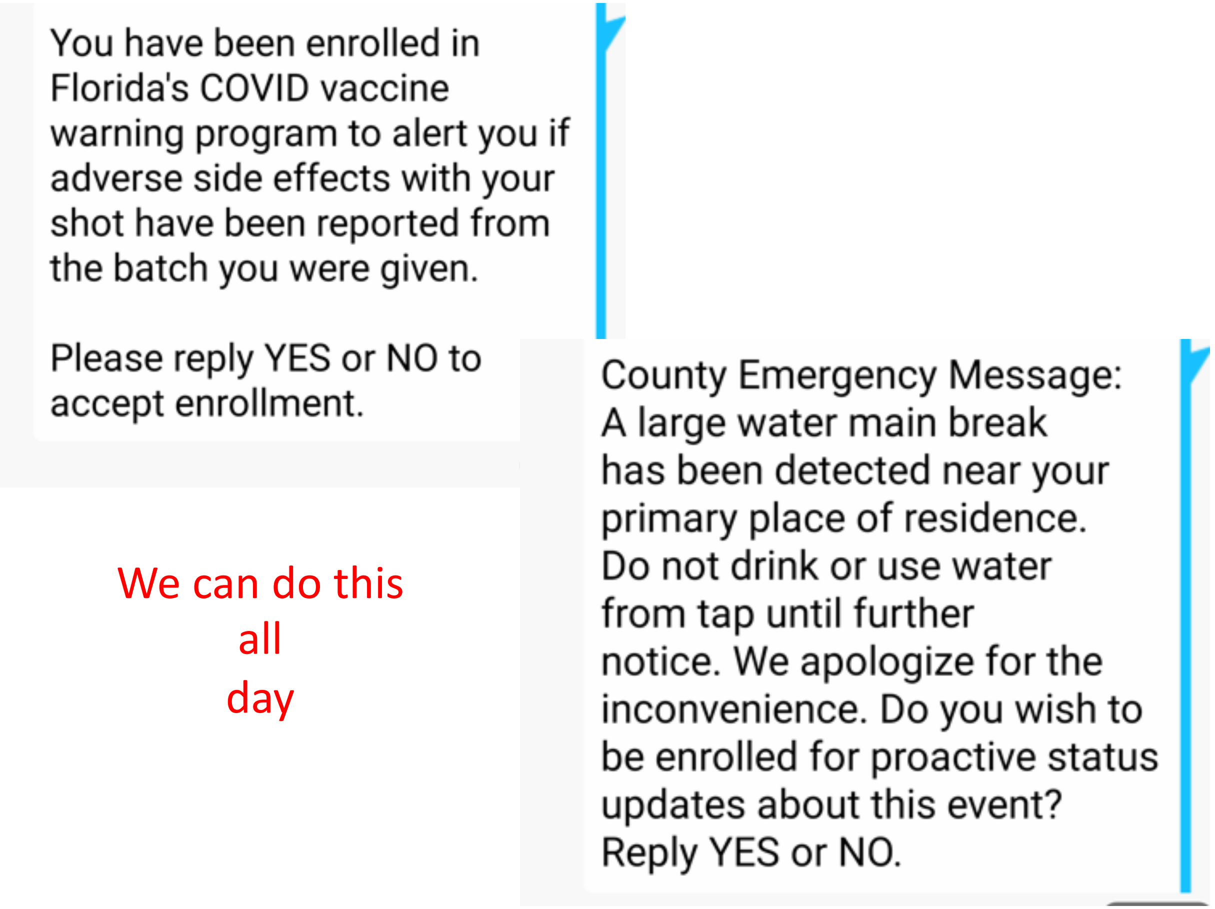
Thank you. Please reply with the confirmation code just sent to confirm your phone number.

357291

Thank you. You are now protected by the NWS emergency warning system. You can stop any time by replying with STOP.

Read

Code from their email, bank account, or stock account being reset →



You have been enrolled in Florida's COVID vaccine warning program to alert you if adverse side effects with your shot have been reported from the batch you were given.

Please reply YES or NO to accept enrollment.

County Emergency Message: A large water main break has been detected near your primary place of residence. Do not drink or use water from tap until further notice. We apologize for the inconvenience. Do you wish to be enrolled for proactive status updates about this event? Reply YES or NO.

We can do this all day

MFA Hacks

SMS Swapping

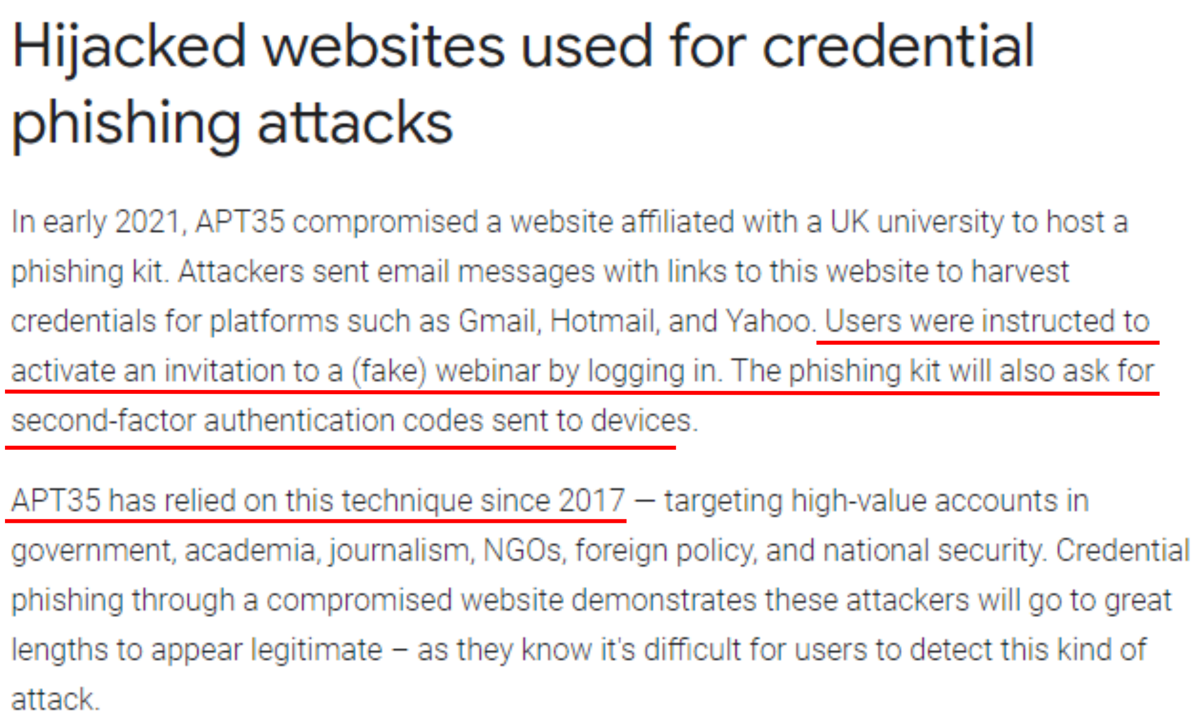
SMS Swapping Attack (con’t)

- Defense: Use non-SMS-based apps
  - App travels with authenticated user, not phone number or SIM
  - Can’t be as easily transferred by 3rd party without your knowledge or participation
  - Not perfect, but stops easy SMS-swapping attacks

Rogue Recoveries

MFA Rogue Recovery

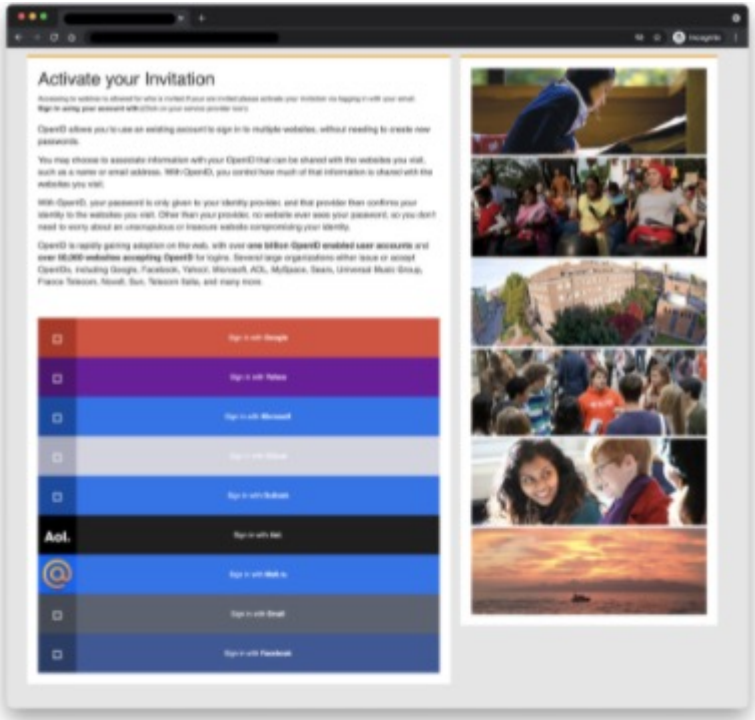
Real Life Hack Example



Hijacked websites used for credential phishing attacks

In early 2021, APT35 compromised a website affiliated with a UK university to host a phishing kit. Attackers sent email messages with links to this website to harvest credentials for platforms such as Gmail, Hotmail, and Yahoo. Users were instructed to activate an invitation to a (fake) webinar by logging in. The phishing kit will also ask for second-factor authentication codes sent to devices.

APT35 has relied on this technique since 2017 — targeting high-value accounts in government, academia, journalism, NGOs, foreign policy, and national security. Credential phishing through a compromised website demonstrates these attackers will go to great lengths to appear legitimate – as they know it's difficult for users to detect this kind of attack.



Phishing page hosted on a compromised website

https://blog.google/threat-analysis-group/countering-threats-iran/

MFA Hacks

Social Engineer Tech Support

- There have been many real-world instances where the user had MFA to a particular web site or service, maybe even required that it be used;
- And hackers socially engineered tech support into disabling it and resetting password, using other information they had learned
- Hackers like to use “stressor” events to achieve their goals
- Humans just want to help, and will bypass policy and controls to do so

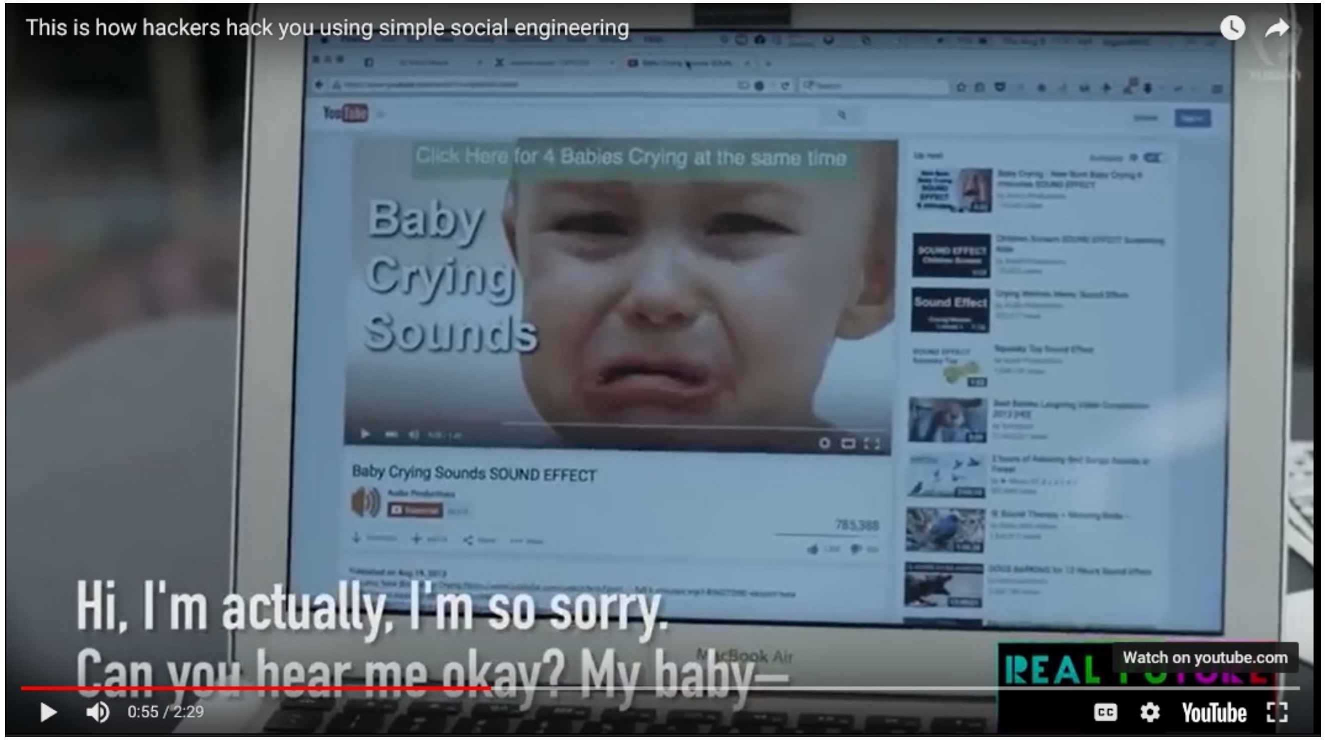
MFA Hacks

Social Engineer Tech Support

Great Example

Check out the “Crying baby” social engineering live demo video:

https://www.youtube.com/watch?v=lc7scxvKQOo

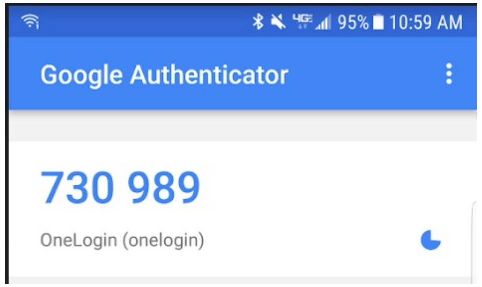


This is how hackers hack you using simple social engineering

Hi, I'm actually, I'm so sorry.
Can you hear me okay? My baby—

MFA Hacks

Duplicate Code Generator



95% 10:59 AM

Google Authenticator

730 989

OneLogin (onelogin)

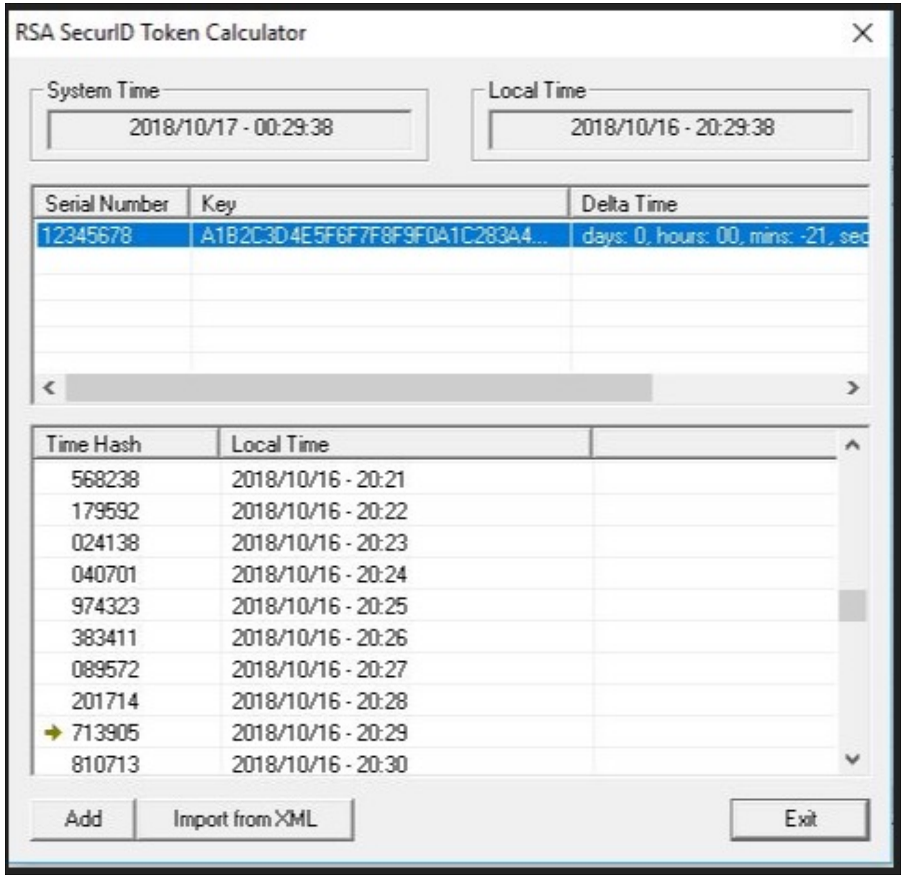
- Most MFA code-generating tokens start with a (randomly) generated (permanently) stored “seed” or “shared secret” value, which is then incremented by some sort of counter/algorithm which generates all subsequent values
  - Known as **one-time passwords** (OTP)
  - “Will never be repeated again”
- Unique user/device identifier usually involved
- May also use current time/date to “randomly” generated code good only for a particular time interval
    - Known as **time-based one-time passwords** (TOTP)

MFA Hacks

Duplicate Code Generator

- Shared secret will always be present in at least two places (e.g. source database/verifier and device itself)
- Attackers that learn seed/shared secret and algorithm can generate duplicate/identical code generators that match the victim's code generator

Taken from Cain & Abel hacking tool



RSA SecurID Token Calculator

System Time: 2018/10/17 - 00:29:38

Local Time: 2018/10/16 - 20:29:38

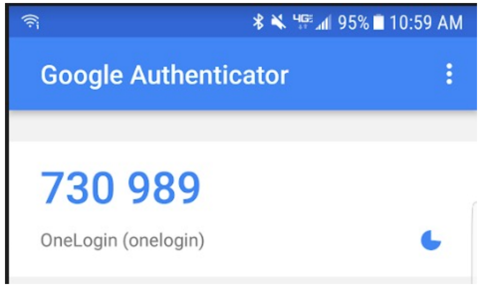
Serial Number	Key	Delta Time
12345678	A1B2C3D4E5F6F7F8F9F0A1C283A4...	days: 0, hours: 00, mins: -21, sec

Time Hash	Local Time
568238	2018/10/16 - 20:21
179592	2018/10/16 - 20:22
024138	2018/10/16 - 20:23
040701	2018/10/16 - 20:24
974323	2018/10/16 - 20:25
383411	2018/10/16 - 20:26
089572	2018/10/16 - 20:27
201714	2018/10/16 - 20:28
→ 713905	2018/10/16 - 20:29
810713	2018/10/16 - 20:30

MFA Hacks

Duplicate Code Generator

- Shared secret will always be present in at least two places (e.g. source database/verifier and device itself)
- Attackers that learn seed/shared secret and algorithm can generate duplicate/identical code generators that match the victim's code generator


95% 10:59 AM

Google Authenticator

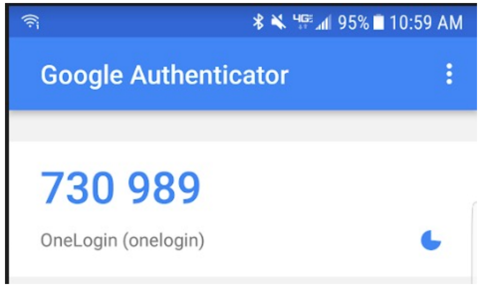
730 989

OneLogin (onelogin)

Real-Life Example: Chinese APT, RSA, and Lockheed Martin attack

MFA Hacks

Duplicate Code Generator

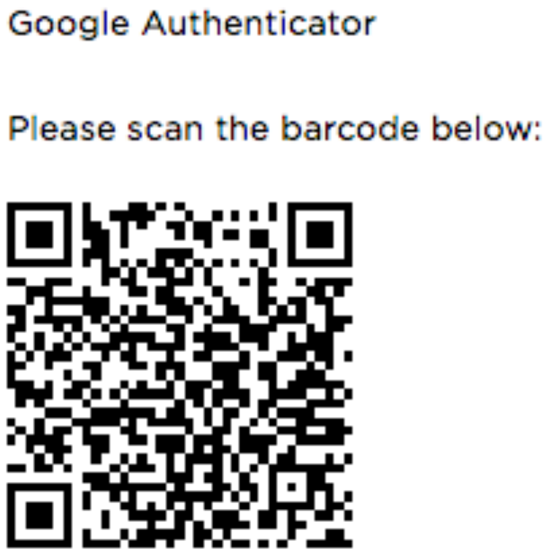


Google Authenticator

730 989

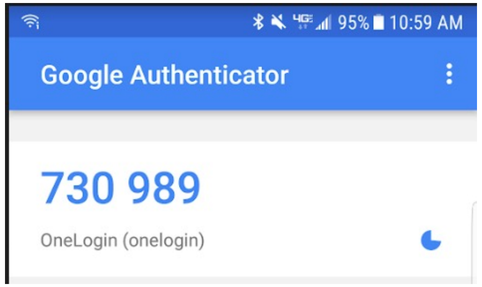
OneLogin (onelogin)

- When you first use Google Authenticator, you will usually be sent a QR code
- It may or may not expire
- That QR code has all the token secrets necessary to create the same Google Authenticator instance
- I can install on multiple devices at the same time (hacker's love this)



Google Authenticator

Please scan the barcode below:



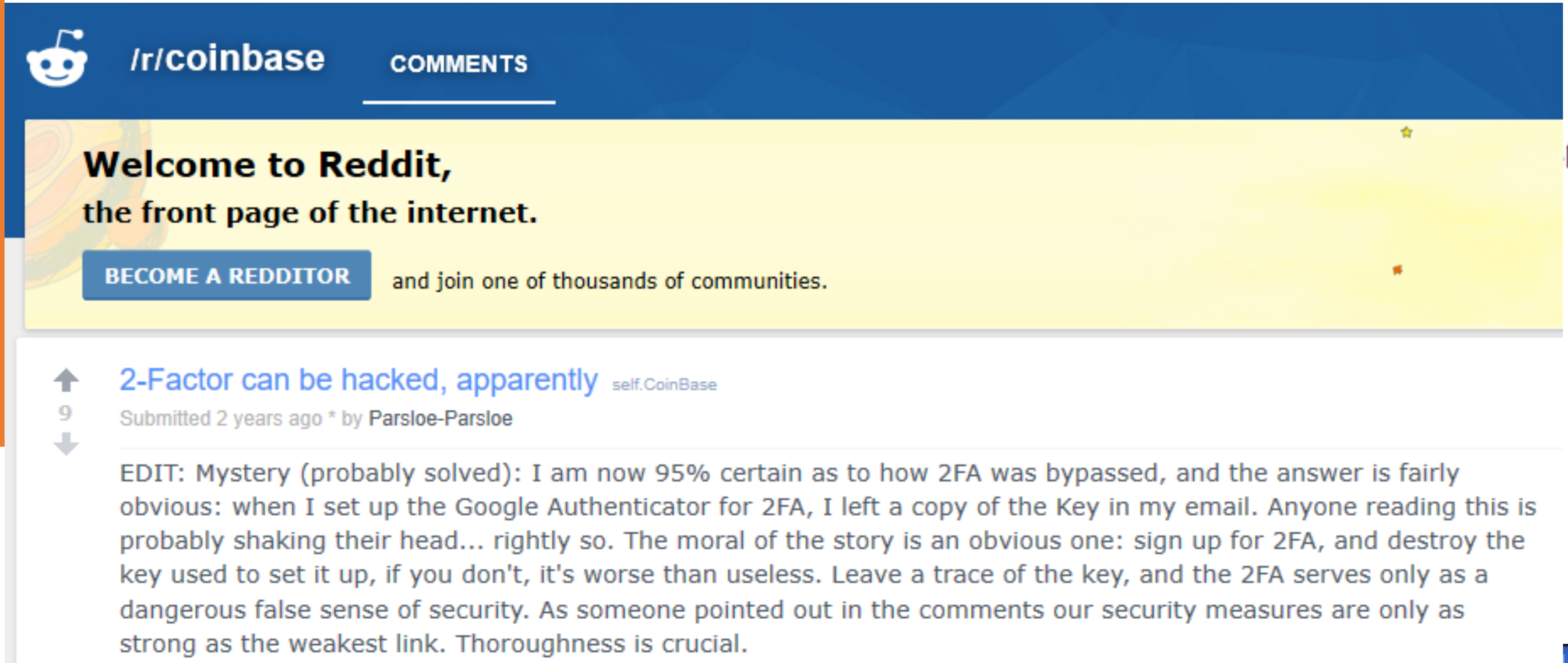
Google Authenticator

730 989

OneLogin (onelogin)

MFA Hacks

Duplicate Code Generator



Welcome to Reddit,

the front page of the internet.

BECOME A REDDITOR and join one of thousands of communities.

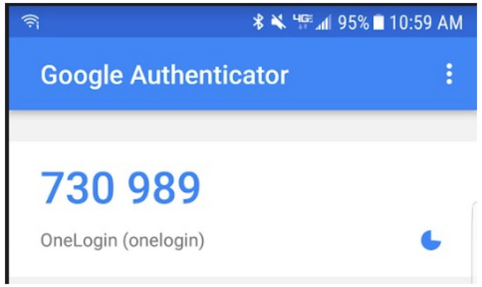
low:

9

2-Factor can be hacked, apparently self.CoinBase

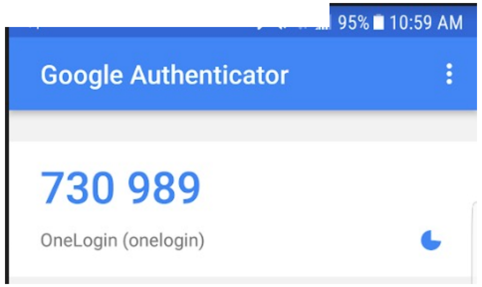
Submitted 2 years ago * by Parsloe-Parsloe

EDIT: Mystery (probably solved): I am now 95% certain as to how 2FA was bypassed, and the answer is fairly obvious: when I set up the Google Authenticator for 2FA, I left a copy of the Key in my email. Anyone reading this is probably shaking their head... rightly so. The moral of the story is an obvious one: sign up for 2FA, and destroy the key used to set it up, if you don't, it's worse than useless. Leave a trace of the key, and the 2FA serves only as a dangerous false sense of security. As someone pointed out in the comments our security measures are only as strong as the weakest link. Thoroughness is crucial.



730 989

OneLogin (onelogin)

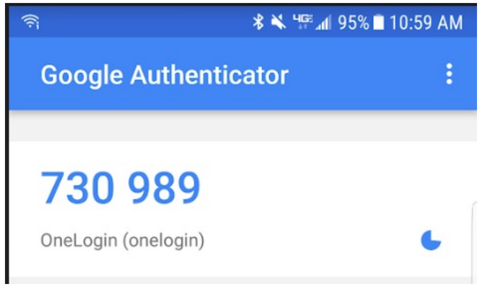


730 989

OneLogin (onelogin)

MFA Hacks

Duplicate Code Generator



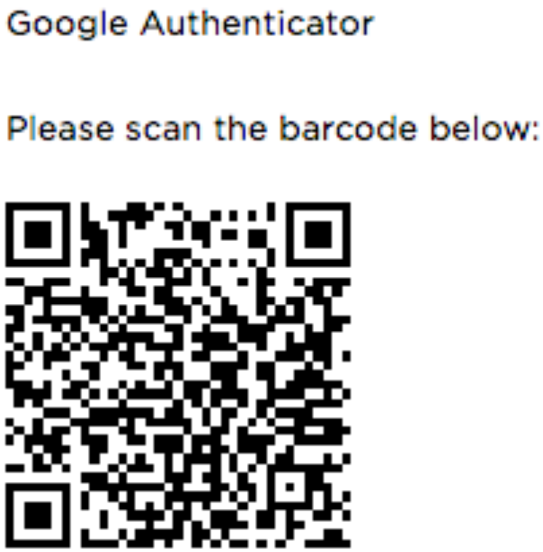
95% 10:59 AM

Google Authenticator

730 989

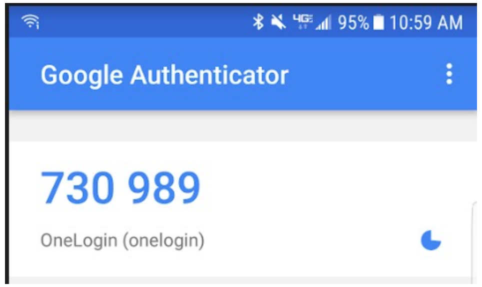
OneLogin (onelogin)

- Google Authenticator uses an 80-bit secret key
- Not that hard to hack
- US gov't says a min. of 128-bit key is required for any TOTP
- I guess it's only a problem if someone knows the Google Authenticator algorithm
- Yeah, turns out, someone does



Google Authenticator

Please scan the barcode below:



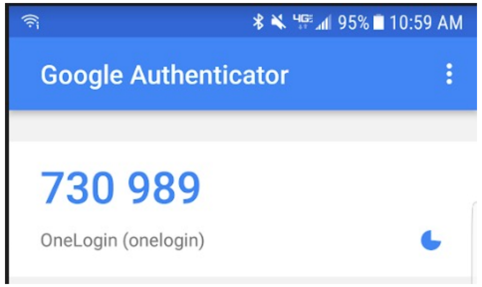
95% 10:59 AM

Google Authenticator

730 989

OneLogin (onelogin)

Duplicate Code Generator

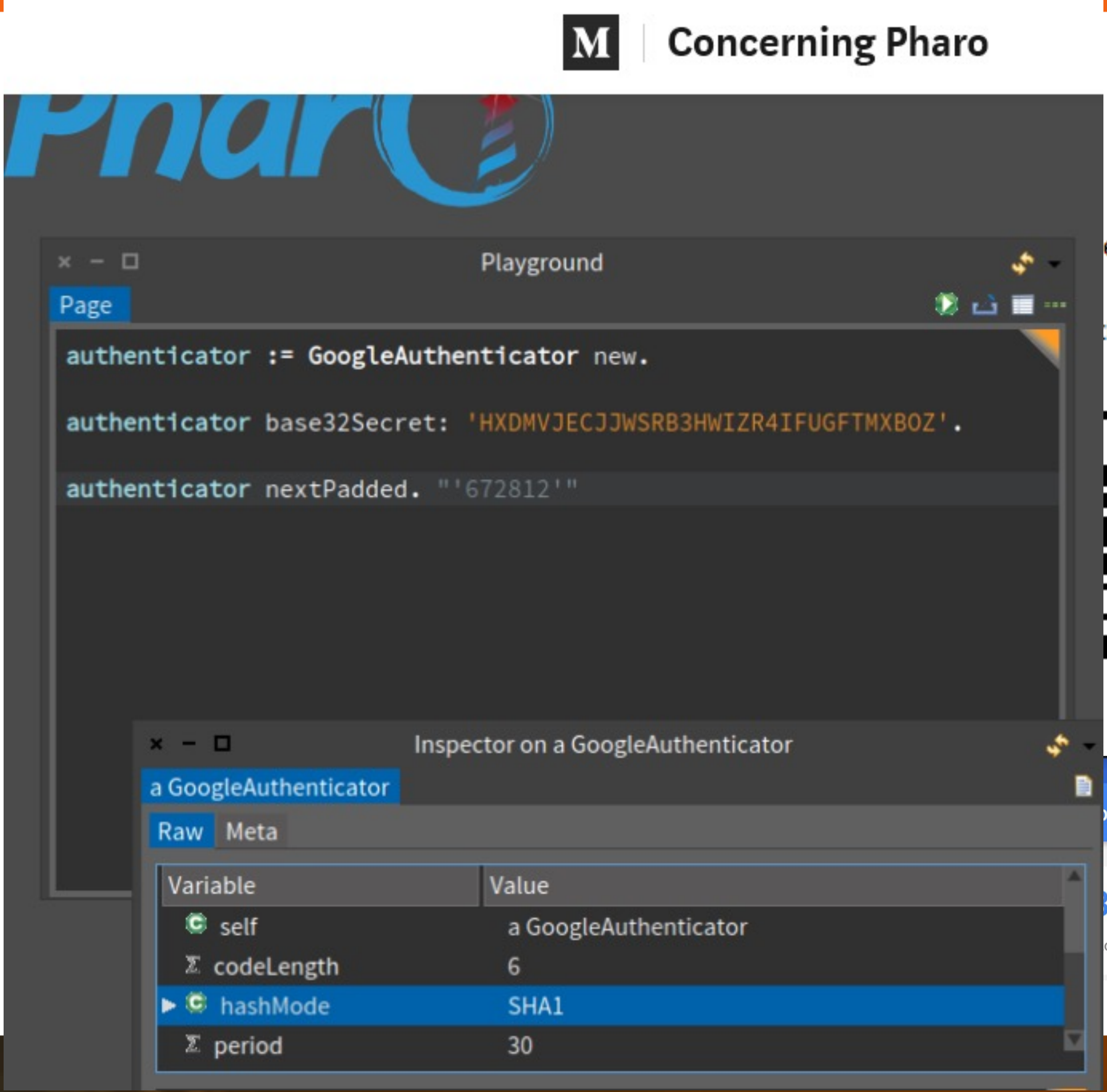


10:59 AM 95%

Google Authenticator

730 989

OneLogin (onelogin)



Concerning Pharo

Playground

```
authenticator := GoogleAuthenticator new.

authenticator base32Secret: 'HXDMVJECJJWSRB3HWIZR4IFUGFTMXBOZ'.

authenticator nextPadded. "'672812'"
```

Inspector on a GoogleAuthenticator

a GoogleAuthenticator

Raw | Meta

Variable	Value
self	a GoogleAuthenticator
codeLength	6
hashMode	SHA1
period	30

enticator

the barcode below:

10:59 AM 95%

gle Authenticator

0 989

ogin (onelogin)

MFA Hacks

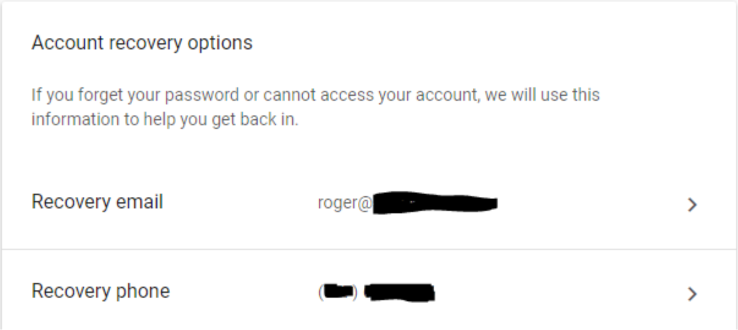
Not Required/ Downgrade Attacks

- If you still have a 1FA solution for a site or service, and it can still be used, then it’s like you don’t really have MFA
- Many sites and services that allow MFA, don’t require it
- If your MFA comes with a non-MFA “master key” or code, then that code can be stolen
- Which means attacker can use non-MFA credential to access
- May allow both more secure and less secure MFA methods, but you likely can’t force only one method

MFA Hacks

Not Required/ Recovery Attacks

- ALL logon recovery methods are far less secure than MFA
- Can bypass many MFA requirements by answering much less secure password reset answers
- Attackers can spoof your registered recovery phone number and automatically be authenticate to some services/voicemail systems

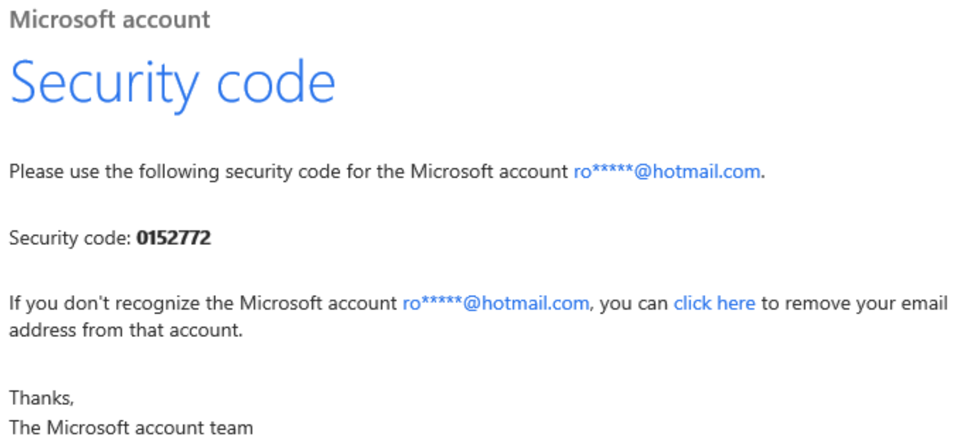


Account recovery options

If you forget your password or cannot access your account, we will use this information to help you get back in.

Recovery email roger@[redacted] ›

Recovery phone ([redacted]) [redacted] ›



Microsoft account

Security code

Please use the following security code for the Microsoft account ro*****@hotmail.com.

Security code: **0152772**

If you don't recognize the Microsoft account ro*****@hotmail.com, you can click here to remove your email address from that account.

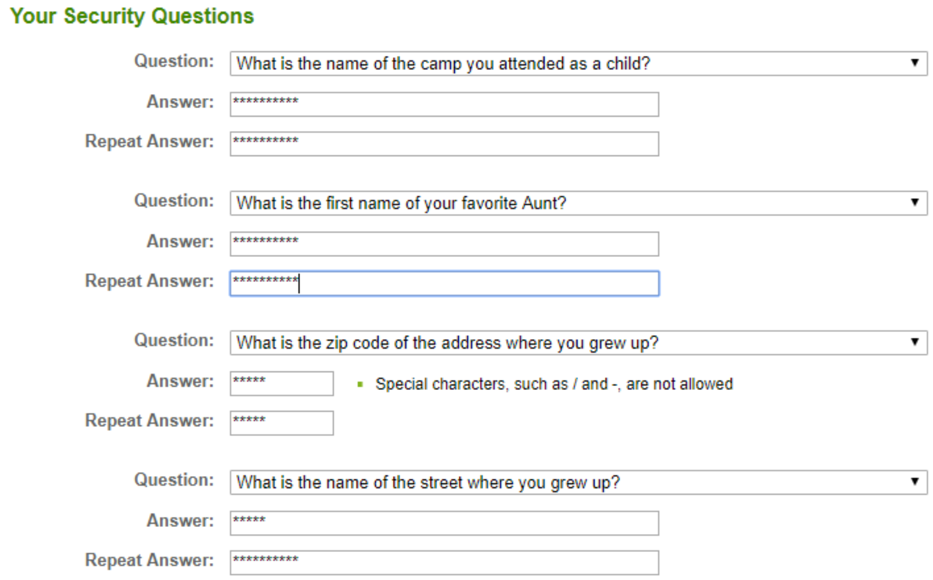
Thanks,
The Microsoft account team

MFA Hacks

Not Required/ Recovery Questions

The worst recovery method on the planet is password recovery questions

- Usually REQUIRED by many web sites, you can't create a new account without them



Your Security Questions

Question:	What is the name of the camp you attended as a child? ▼
Answer:	**********
Repeat Answer:	**********
Question:	What is the first name of your favorite Aunt? ▼
Answer:	**********
Repeat Answer:	**********
Question:	What is the zip code of the address where you grew up? ▼
Answer:	***** ▪ Special characters, such as / and -, are not allowed
Repeat Answer:	*****
Question:	What is the name of the street where you grew up? ▼
Answer:	*****
Repeat Answer:	**********

MFA Hacks

Not Required/ Recovery Questions

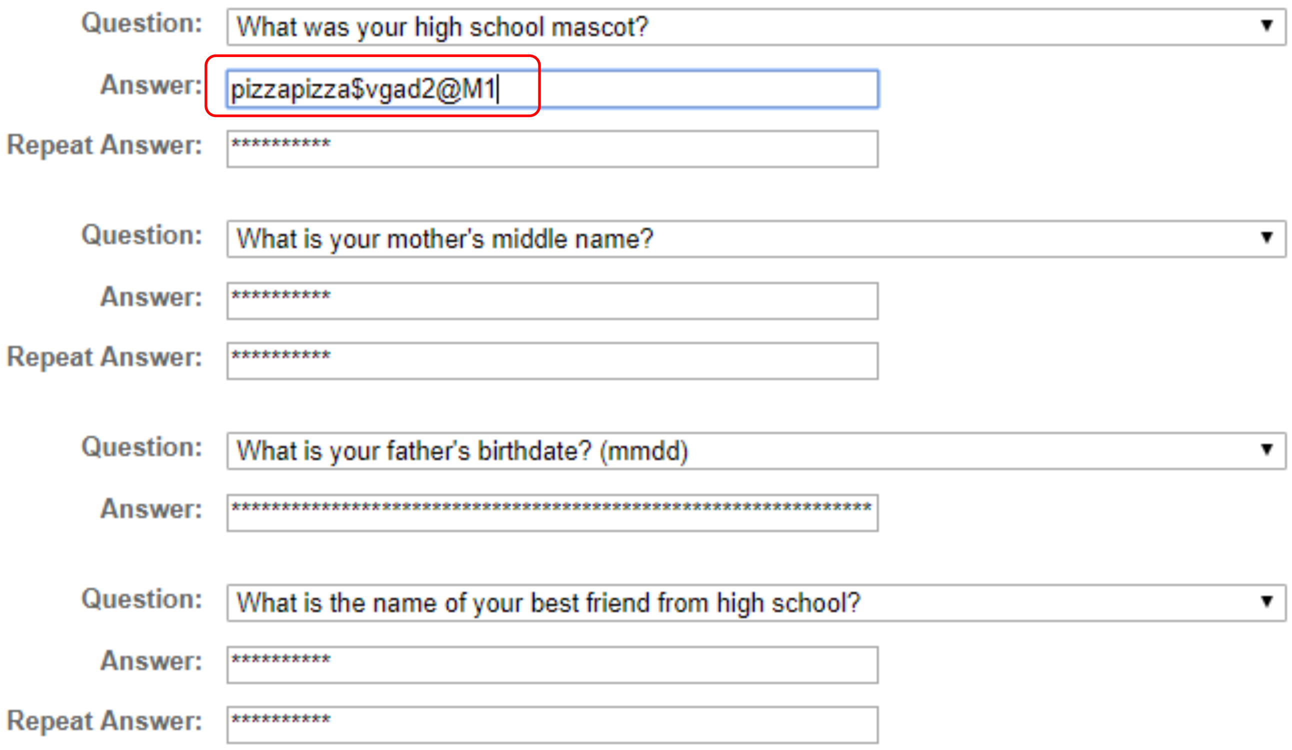
Problem: Answers can often be easily guessed by hackers

- Great Google paper called *Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google*
  - http://www.a51.nl/sites/default/files/pdf/43783.pdf
  - For example, some recovery questions can be guessed on first try 20% of the time
  - 40% of people were unable to successfully recall their own recovery answers
  - 16% of answers could be found in person’s social media profile
- Attack has been involved in many well known attacks (e.g. Sarah Palin’s compromised email)

MFA Hacks

Not Required/ Recovery Questions

Solution: Never answer the questions with the real answers!



Question: What was your high school mascot? ▾

Answer: pizzapizza$vgad2@M1

Repeat Answer: **********

Question: What is your mother's middle name? ▾

Answer: **********

Repeat Answer: **********

Question: What is your father's birthdate? (mmdd) ▾

Answer: ***

Question: What is the name of your best friend from high school? ▾

Answer: **********

Repeat Answer: **********

Unfortunate that means you have to record them somewhere else just like passwords (password managers help with this)

MFA Hacks

Reuse Stolen Biometrics

- If your biometric identity is stolen, how do you stop a bad guy from re-using it?
- Once stolen, it’s compromised for your life
- You can change a password or smartcard, you can’t easily change your retina scan or fingerprint
- Known as non-repudiation attack in the crypto world
- Attacker might even steal your biometric attribute (e.g. finger/hand) to reuse
- But more likely to steal in digital form and replay

Example: June 2015 OPM attack stole biometrics of 5.6 million people

MFA Hacks

Reuse Stolen Biometrics

Another example:

- Aug. 2019 breach
- Biostar2 platform
- Fingerprints and facial recog
- Top 50 biometric app vendor
- Over 1 million fingerprints breached
- The breachers claim company was largely unresponsive and uncooperative to their reports and ongoing discussions

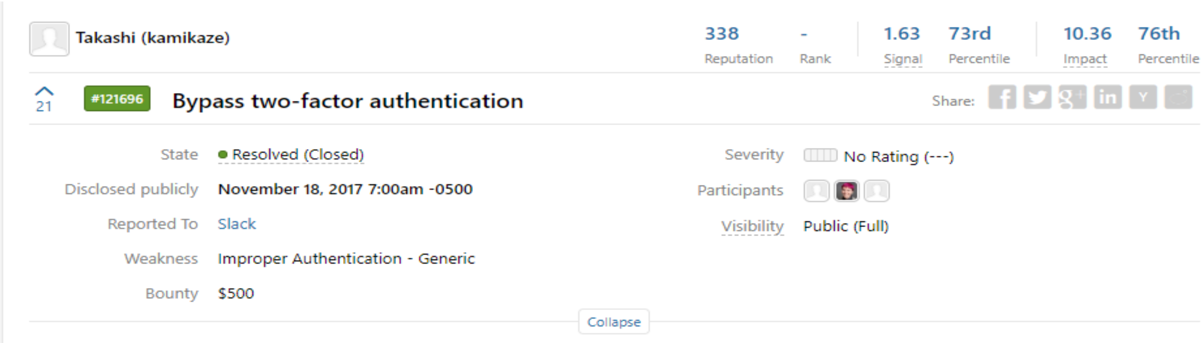
Report: Data Breach in Biometric Security Platform Affecting Millions of Users

Biostar 2 Breach: Millions of Users Exposed in Huge Data Leak
vpnMentor

MFA Hacks

Brute Force

- If the MFA auth screen doesn't include account lockouts for x


Takashi (kamikaze)

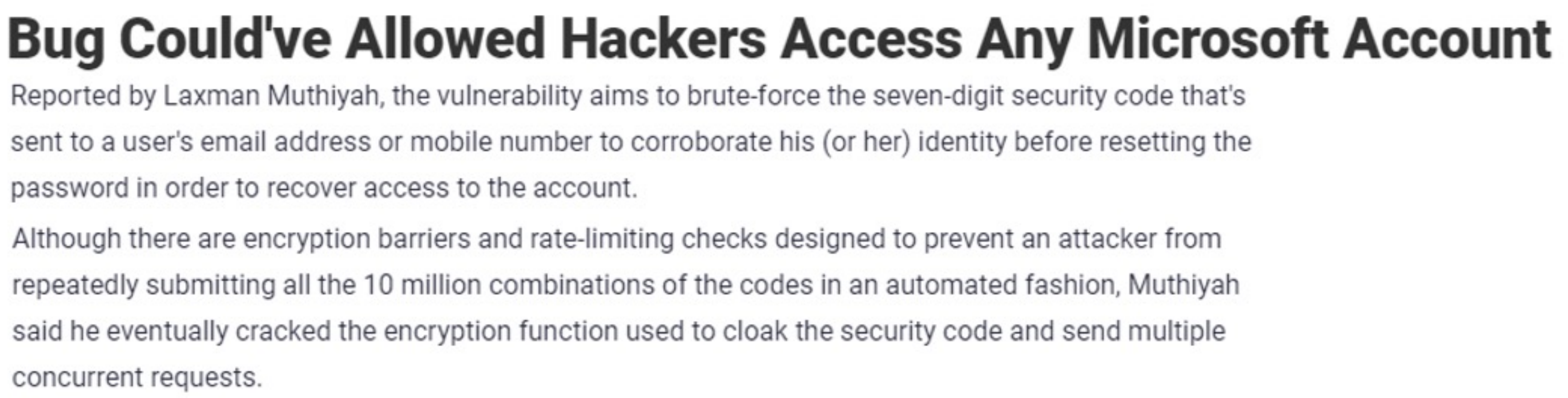
338	-	1.63	73rd	10.36	76th
Reputation	Rank	Signal	Percentile	Impact	Percentile

21 #121696 Bypass two-factor authentication

Share:

State	Resolved (Closed)	Severity	No Rating (---)
Disclosed publicly	November 18, 2017 7:00am -0500	Participants	
Reported To	Slack	Visibility	Public (Full)
Weakness	Improper Authentication - Generic		
Bounty	$500		

Researcher Bypass


Bug Could've Allowed Hackers Access Any Microsoft Account

Reported by Laxman Muthiyah, the vulnerability aims to brute-force the seven-digit security code that's sent to a user's email address or mobile number to corroborate his (or her) identity before resetting the password in order to recover access to the account.

Although there are encryption barriers and rate-limiting checks designed to prevent an attacker from repeatedly submitting all the 10 million combinations of the codes in an automated fashion, Muthiyah said he eventually cracked the encryption function used to cloak the security code and send multiple concurrent requests.

Mar 9th (2 years ago)

ıy times" because your bug

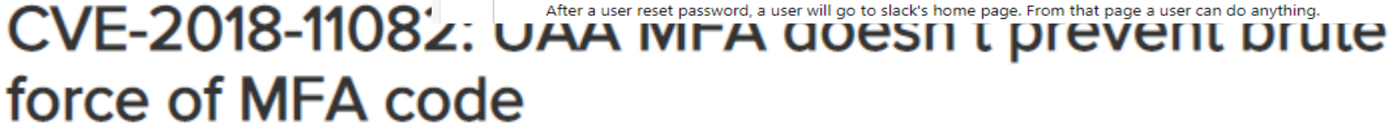
ɹn't use any automated tools

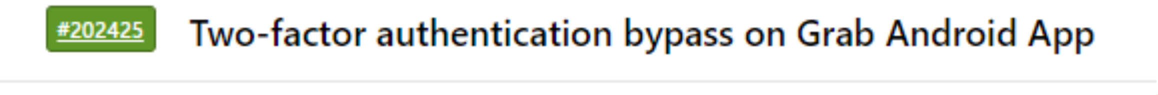
ɾce attacks

- Happens all the ti

By Sergiu Gatlan November 26, 2020

After a user reset password, a user will go to slack's home page. From that page a user can do anything.

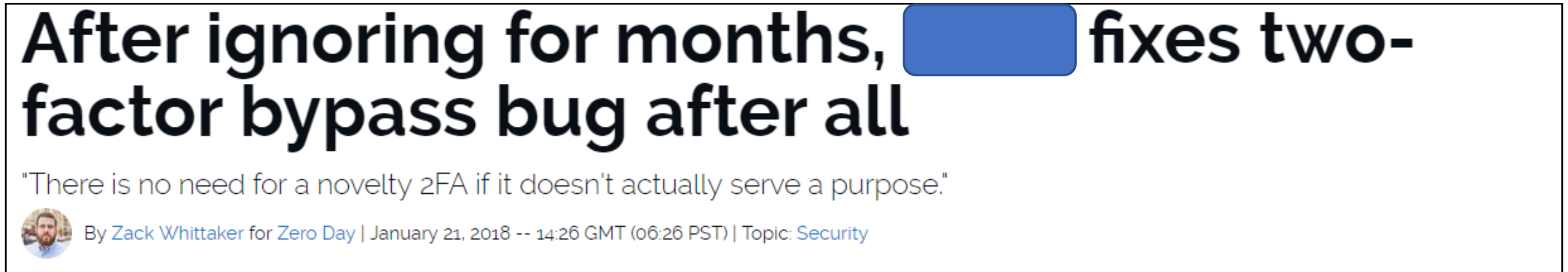

CVE-2018-11082: UAA MFA doesn't prevent brute force of MFA code


#202425 Two-factor authentication bypass on Grab Android App

MFA Hacks

Buggy MFA

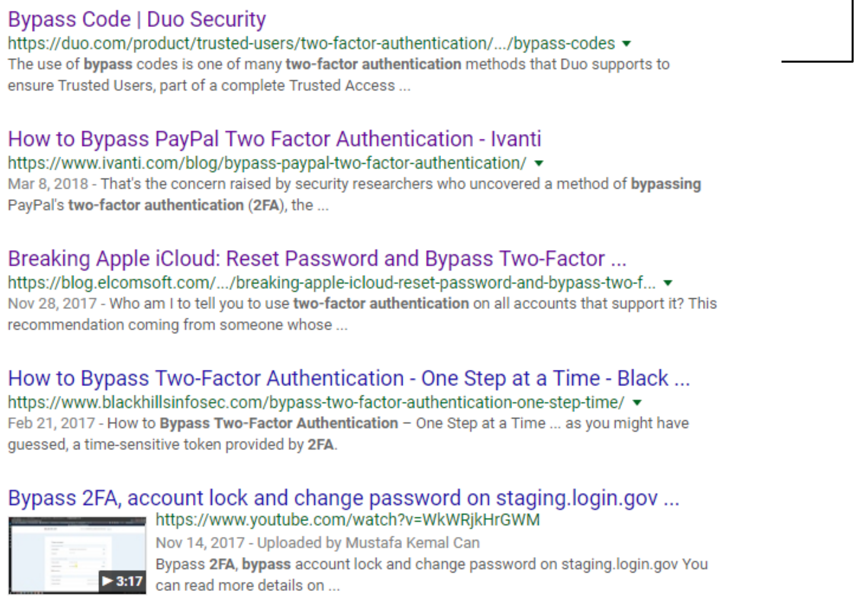
- Bugs are bugs, some bypass MFA



After ignoring for months, [redacted] fixes two-factor bypass bug after all

"There is no need for a novelty 2FA if it doesn't actually serve a purpose."

By Zack Whittaker for Zero Day | January 21, 2018 -- 14:26 GMT (06:26 PST) | Topic: Security



Bypass Code | Duo Security
https://duo.com/product/trusted-users/two-factor-authentication/.../bypass-codes ▾
The use of **bypass** codes is one of many **two-factor authentication** methods that Duo supports to ensure Trusted Users, part of a complete Trusted Access ...

How to Bypass PayPal Two Factor Authentication - Ivanti
https://www.ivanti.com/blog/bypass-paypal-two-factor-authentication/ ▾
Mar 8, 2018 - That's the concern raised by security researchers who uncovered a method of **bypassing** PayPal's **two-factor authentication** (**2FA**), the ...

Breaking Apple iCloud: Reset Password and Bypass Two-Factor ...
https://blog.elcomsoft.com/.../breaking-apple-icloud-reset-password-and-bypass-two-f... ▾
Nov 28, 2017 - Who am I to tell you to use **two-factor authentication** on all accounts that support it? This recommendation coming from someone whose ...

How to Bypass Two-Factor Authentication - One Step at a Time - Black ...
https://www.blackhillsinfosec.com/bypass-two-factor-authentication-one-step-time/ ▾
Feb 21, 2017 - How to **Bypass Two-Factor Authentication** – One Step at a Time ... as you might have guessed, a time-sensitive token provided by **2FA**.

Bypass 2FA, account lock and change password on staging.login.gov ...
▶ 3:17
https://www.youtube.com/watch?v=WkWRjkHrGWM
Nov 14, 2017 - Uploaded by Mustafa Kemal Can
Bypass **2FA**, **bypass** account lock and change password on staging.login.gov You can read more details on ...

MFA Hacks

Buggy MFA

2017 ROCA vulnerability

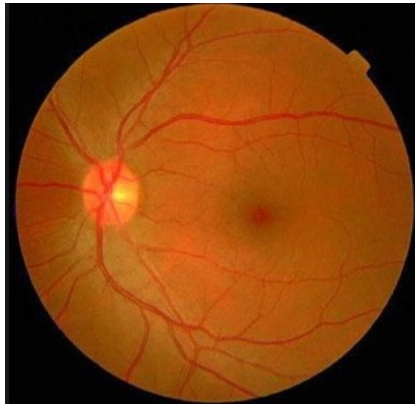
- Sometimes a single bug impacts hundreds of millions of otherwise unrelated MFA devices
- Huge bug making any MFA product (smartcards, TPM chips, Yubikeys, etc.) with Infineon-generated RSA key lengths of 2048 or smaller (which is most of them), easy to extract the PRIVATE key from public key.
- Still tens to hundreds of millions of devices impacted

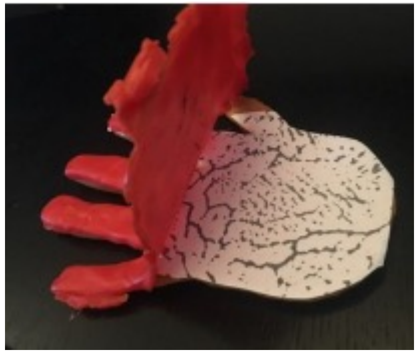
MFA Hacks

Physical Attacks

Biometric

- Fake fingerprints, fake faces, etc.
  - Biometric vendors try to prevent fakes, but hackers just get around
- Stolen and replayed



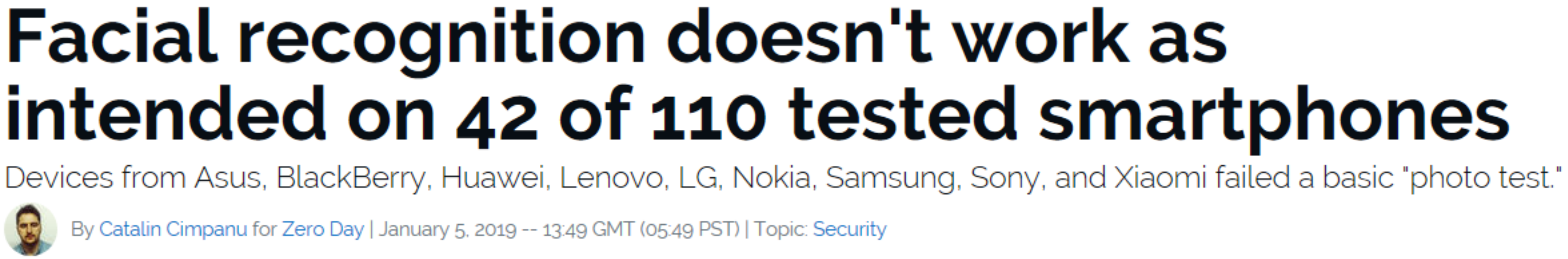


MFA Hacks

Physical Attacks

Biometric – Fake Faces

- Pictures
- 3D Masks
- Photoshopped blinking eyelids in animated gifs



Facial recognition doesn't work as intended on 42 of 110 tested smartphones

Devices from Asus, BlackBerry, Huawei, Lenovo, LG, Nokia, Samsung, Sony, and Xiaomi failed a basic "photo test."

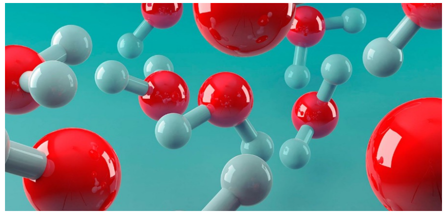
By Catalin Cimpanu for Zero Day | January 5, 2019 -- 13:49 GMT (05:49 PST) | Topic: Security

MFA Hacks

Physical Attacks

TPM Attacks

- Electron microscope can find private key on TPM chips



- Regular, computer cleaning canned air can be used to “freeze” regular RAM memory chips, so that private keys can be extracted
    - Bypasses all disk encryption products

Lessons and Recommendations

Key Takeaways

Lessons

- MFA isn't unhackable
- MFA does not prevent phishing or social engineering from being successful
- MFA is good. Everyone should use it when they can, but it isn't unbreakable
- Try to use/buy phishing-resistant MFA whenever you have to use MFA (if you have a choice)

Hacking MFA

Try to avoid any MFA solution that can be easily social engineered or man-in-the-middle around

Unfortunately, this is most MFA solutions

Hacking MFA

US Gov't Has Said since 2017 Not to Use Easily Hackable MFA

Digital Identity Guidelines, NIST Special Publication 800-63

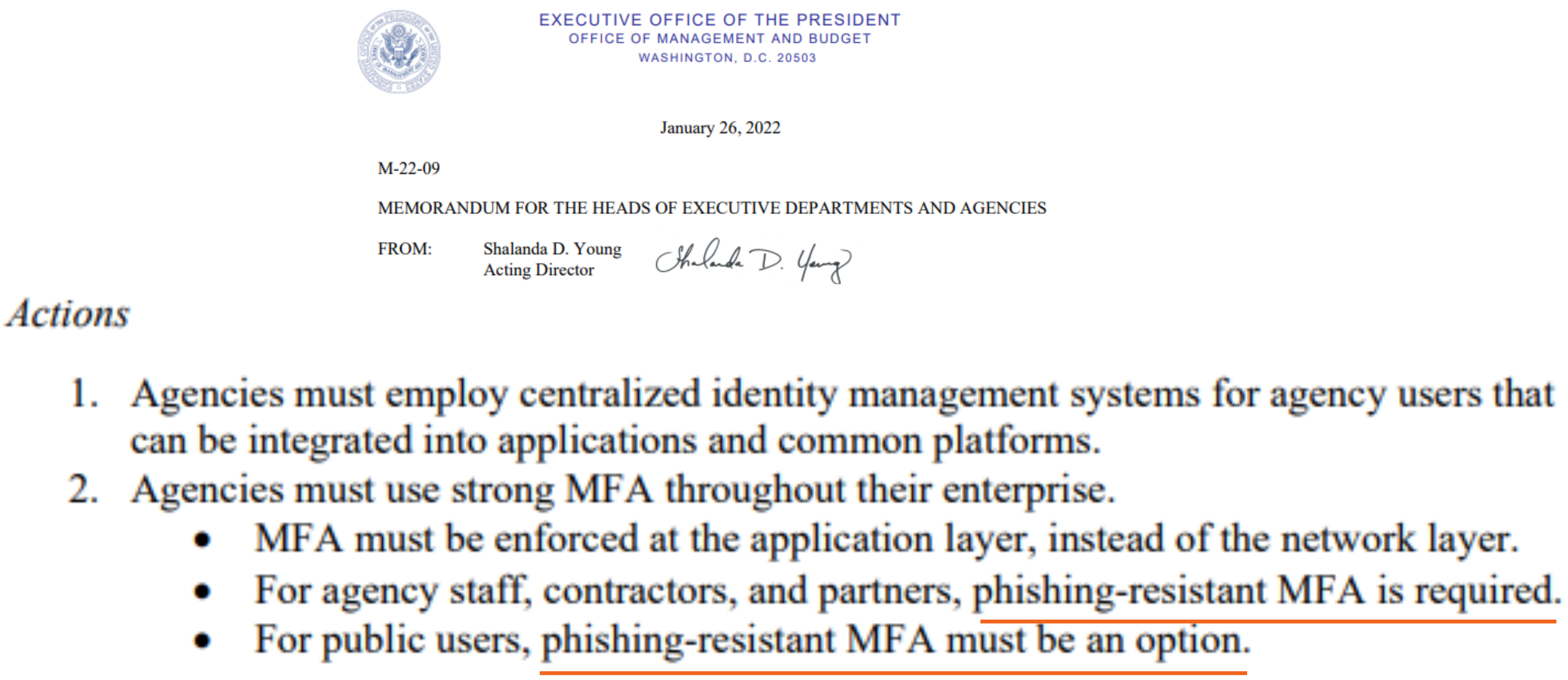
(https://www.nist.gov/itl/applied-cybersecurity/tig/projects/special-publication-800-63)

- States the "Use of the PSTN [Public Switched Telephone Network or a phoneline connection in human-speak] for out-of-band [authentication] verification is RESTRICTED".
  - This means any authentication, including MFA that relies on your phone or phone number as part of its authentication, is "restricted" [i.e., not that secure]. This includes all SMS- and voice call-based MFA.
- In 2021, **Presidential executive order (EO 14028)** had a clarifying follow-up memo (https://zerotrust.cyber.gov/federal-zero-trust-strategy/#identity) that stated, "For routine self-service access by agency staff, contractors and partners, agency systems *must discontinue support* [emphasis added] for authentication methods that *fail to resist phishing*, such as protocols that register phone numbers *for SMS or voice calls, supply one-time codes, or receive push notifications.* [emphasis added]"

Hacking MFA

US Gov't 2022

- **OMB Memo M-22-09 released on January 26, 2022**



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

Shalanda D. Young

Actions

1. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.
2. Agencies must use strong MFA throughout their enterprise.
   - MFA must be enforced at the application layer, instead of the network layer.
   - For agency staff, contractors, and partners, phishing-resistant MFA is required.
   - For public users, phishing-resistant MFA must be an option.

- https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Defending MFA

Parting Thoughts – Education is Necessary

No matter which type of MFA you choose, educate everyone:

- Buyers, Evaluators, Implementors, Users, Senior management

Topics:

- Strengths and weaknesses
- How to correctly use the MFA solution
  - Including what might indicate a malicious attempt to abuse it
  - And what to do during rogue attacks
- What MFA does and doesn't prevent
- The common possible attacks for that type of MFA and how to prevent

- You wouldn't give people passwords without warning them about common hacker tricks

Defending MFA

Use Phishing-Resistant MFA

- **Don't Use Easily Phishable MFA and That's Most MFA!**
- https://www.linkedin.com/pulse/dont-use-easily-phishable-mfa-thats-most-roger-grimes

- **My List of Good, Strong MFA**
- https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes

- **US Government Says to Avoid Phishing-Resistant MFA and Why Is the Majority of Our MFA So Phishable?**
- https://www.linkedin.com/pulse/why-majority-our-mfa-so-phishable-roger-grimes

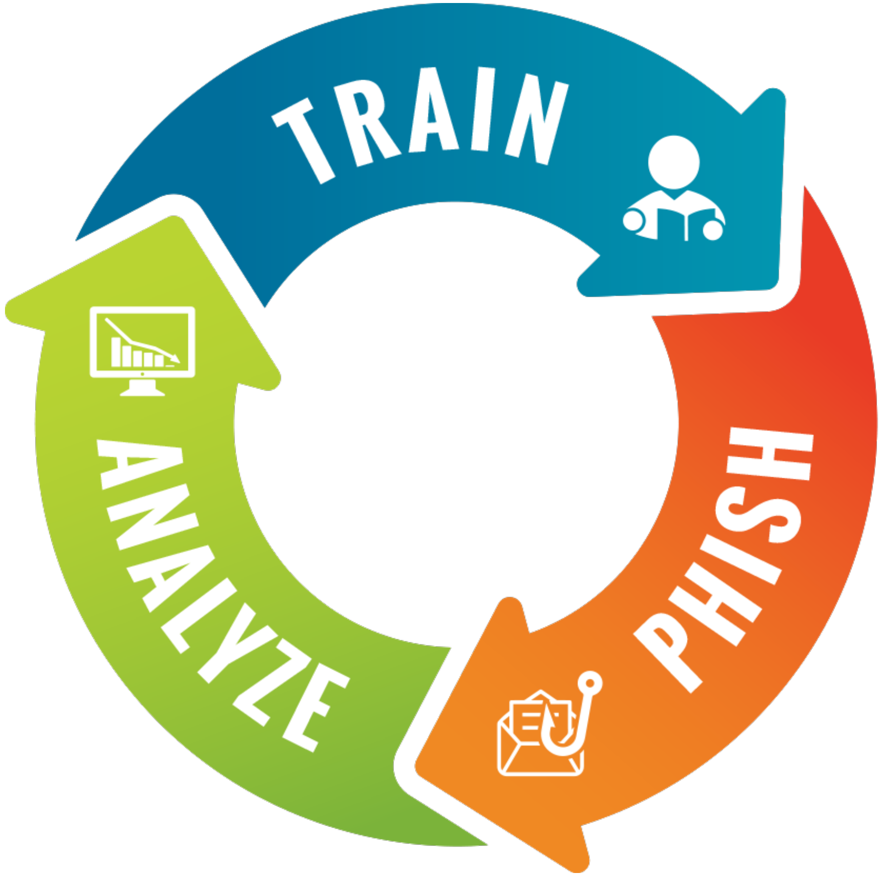
KnowBe4 Security Awareness Training

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

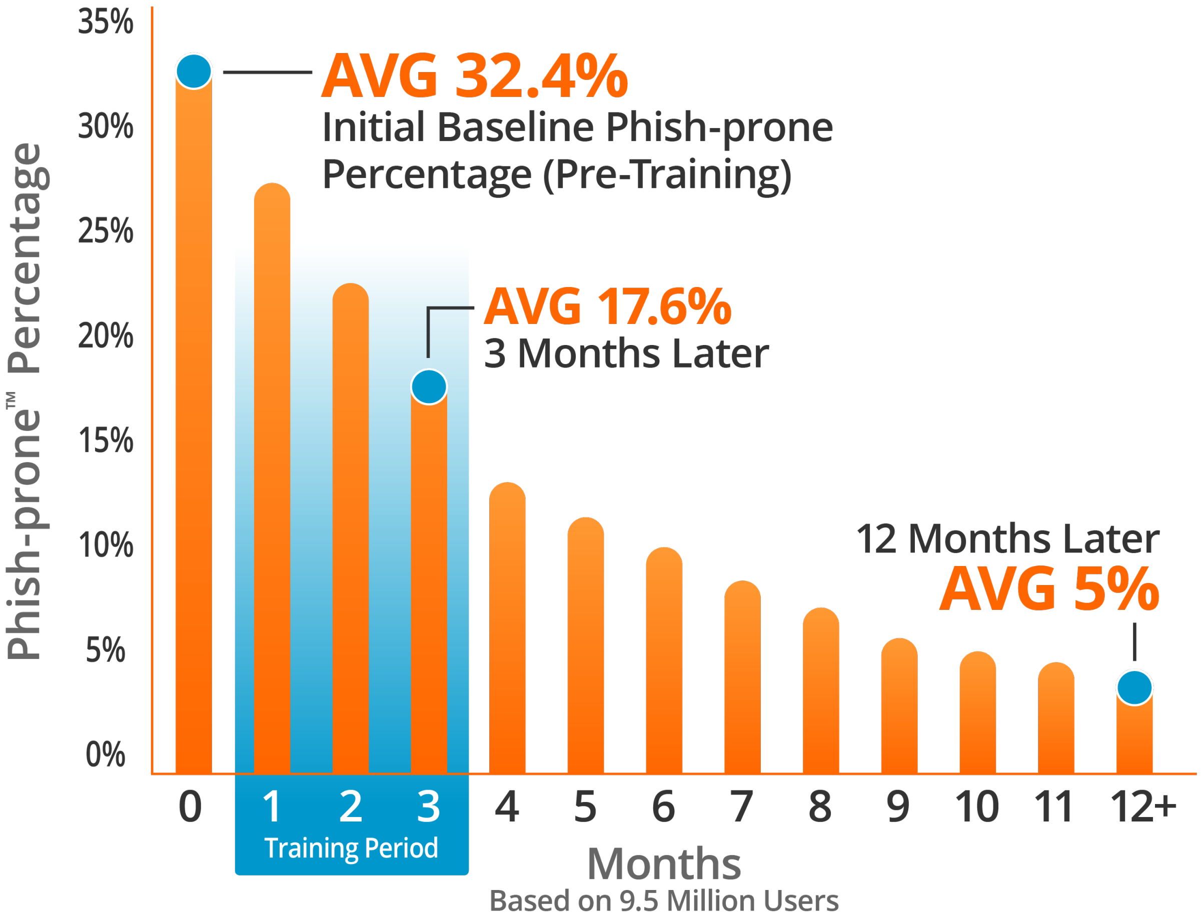


Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

85% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com