KB4-CON

12 Ways to Hack 2FA

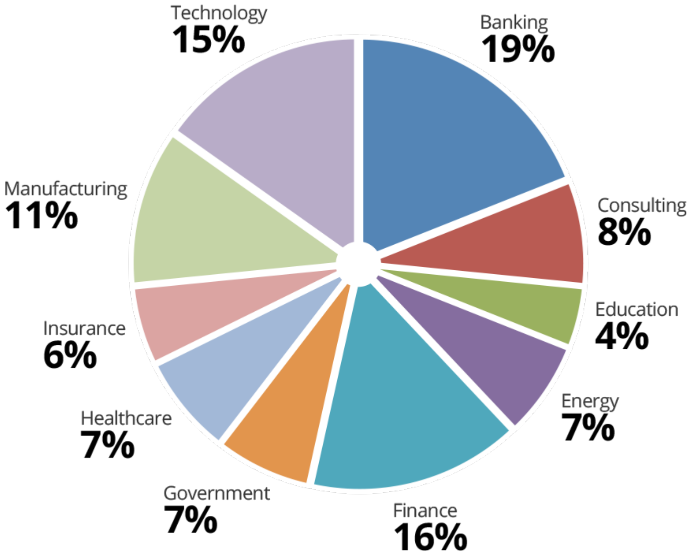
by Roger A. Grimes, Data-Driven Defense Evangelist

e: rogerg@knowbe.com

KnowBe4

KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



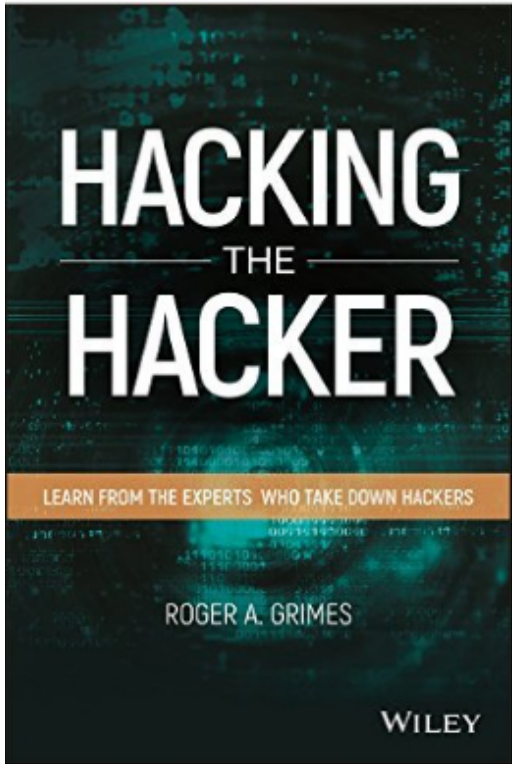
About Roger

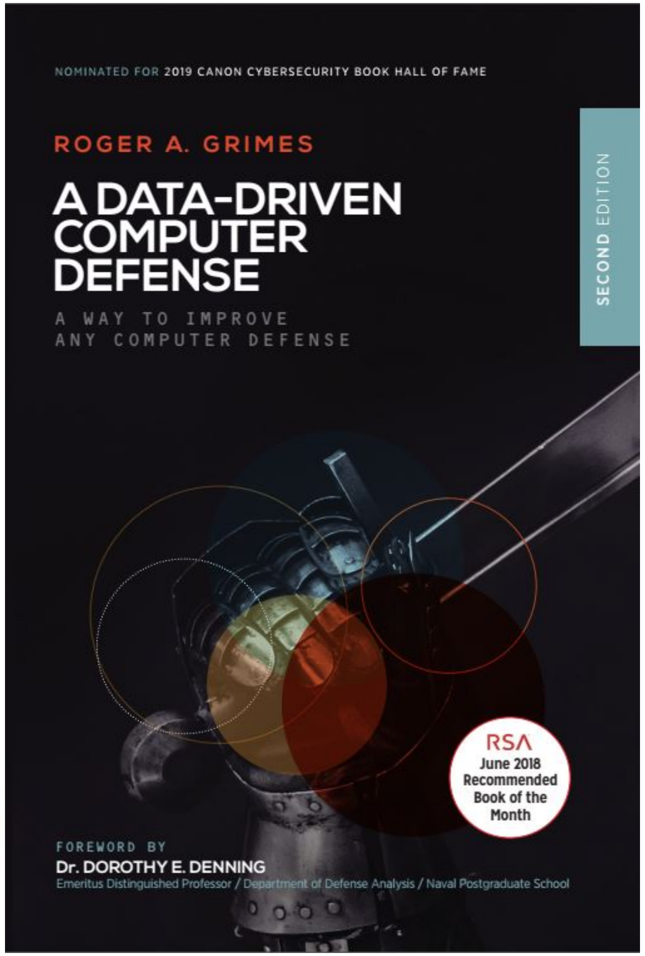
- 30-years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- PKI, smartcards, MFA, biometrics, since 1998
- Consultant to world's largest and smallest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 10 books and over 1000 magazine articles
- InfoWorld and CSO weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

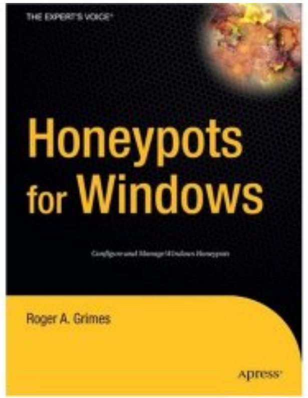
Certifications passed include:

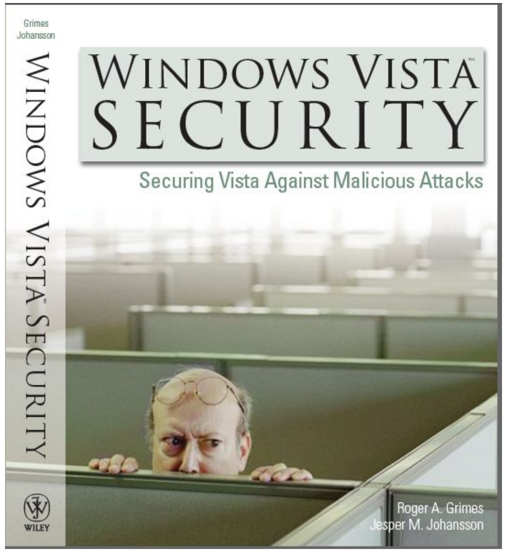
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

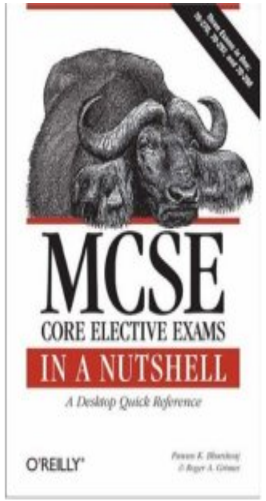
Roger’s Books

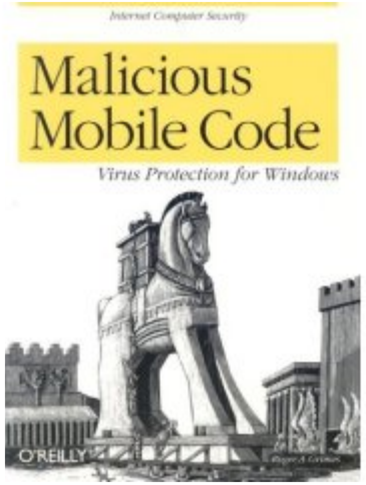


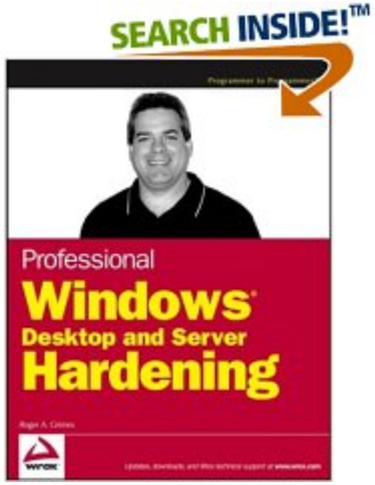

NOMINATED FOR 2019 CANON CYBERSECURITY BOOK HALL OF FAME
ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
SECOND EDITION
RSA June 2018 Recommended Book of the Month
FOREWORD BY
Dr. DOROTHY E. DENNING
Emeritus Distinguished Professor / Department of Defense Analysis / Naval Postgraduate School

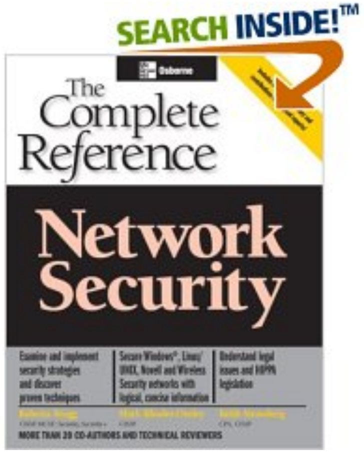


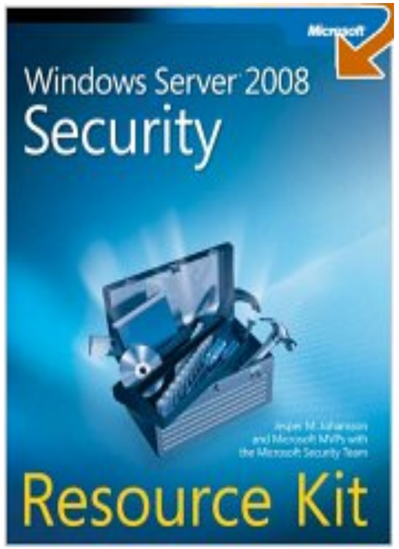











Microsoft
Windows Server 2008
Security
Jesper M. Johansson and Microsoft MVPs with the Microsoft Security Team
Resource Kit

RSA June 2018 Book of the Month

Harvard Business Review

2019 Canon Cybersecurity Book Hall of Fame nominee

What is a Data-Driven Defense Evangelist?

Using data-driven, risk analytics, I want to help companies put:

- The right defenses,
- In the right places,
- In the right amounts,
- Against the right threats

Today’s Presentation

- Multi-Factor Authentication Intro
- Hacking MFA
- Defending Against MFA Attacks

Multi-Factor Authentication Intro

Introduction to Multi-Factor 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
- Behavioral analytics, actions, location, etc.

Introduction to Multi-Factor Authentication

Factors

- Single Factor
- Two Factor (2FA)
- Multi-Factor (MFA)
  - 2-3 factors

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

Introduction to Multi-Factor Authentication

Main MFA Types

Implementation in:

- **“In-Band”**
  - Factor sent/validated using same channel as your authentication access check/app
- **“Out-of-Band”**
  - Factor sent/validated using separate communication channel

Introduction to Multi-Factor Authentication

Auth vs. Auth

1-way vs. 2-way

Authentication can be:

- **One-way**
  - server-only or client-only
  - Most common type
  - Vast majority of web sites use one-way authentication, where server has to prove its identity to client before client will conduct business with it
- **Two-way (mutual)**
  - Both server and client must authenticate to each other
  - Not as common, but more secure
  - Two-way may use different auth methods and/or factors for each side

Introduction to Multi-Factor Authentication

Factors

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

First, we need to understand some basic concepts to better understand hacking MFA

Introduction to Multi-Factor Authentication

Auth vs. Auth

- **Identifier/Identity**
  - Unique label within a common namespace
    - indicates a specific account/subject/user/device/group/service/daemon, etc.
- **Authentication**
  - Process of providing one or more factors that only the subject knows, thus proving ownership and control of the identity
- **Authorization**
  - Process of comparing the now authenticated subject's **access (token)** against previously permissioned/secured resources to determine subject access

Introduction to Multi-Factor Authentication

Auth vs. Auth

Hugely Important Point to Understand

- No matter how I authenticate (e.g. one-factor, multi-Factor, biometrics, etc.), rarely does the authorization use the same authentication token
  - They are completely different processes, often not linked at all to each other
  - Many MFA hacks are based on this delineation

For example

- Even if I authentication to Microsoft Windows using biometrics or a smartcard, after I successfully authenticate, an LM, NTLM, or Kerberos token is used for authorization/access control
- No matter how I authenticate to a web site, the authorization token is likely to be a text-based cookie (e.g. session token)

Hacking MFA

MFA Hacks

General

Main Hacking Methods

- **Social Engineering**
- **Technical Attack** against underlying technology
- **Physical** (biometric theft, etc.)

- Some of the attacks involve two or all methods
- Often insecure transitioning between linked steps (e.g. identity, authentication, and authorization)

Some MFA solutions are better than others, but there is no such thing as "unhackable"

MFA Hacks

Session Hijacking

Three Major Session Hijacking Methods

Session hijacking can be accomplished using a variety of different methods, including session token:

- Reproduction/Guessing
  - Often through prediction of the session’s unique identifier
- Theft of session access token at the end-point
- Theft of session access token in the network communication channel

MFA Hacks

Network Session Hijacking

- Usually requires Man-in-the-Middle (MitM) attacker
- Attacker puts themselves inside of the communication stream between legitimate sender and receiver
- Doesn’t usually care about authentication that much
- Just wants to steal resulting, legitimate access session token after successful authentication
- On web sites, session tokens are usually represented by a “cookie” (a simple text file containing information unique for the user/device and that unique session)
- Session token usually just good for session

MFA Hacks

Network Session Hijacking

Session Hijacking Proxy Theft

Use Rogue Proxy/Server to:

- Replay and Steal Credentials
- Steal Session Cookie

MFA Hacks

Network Session Hijacking

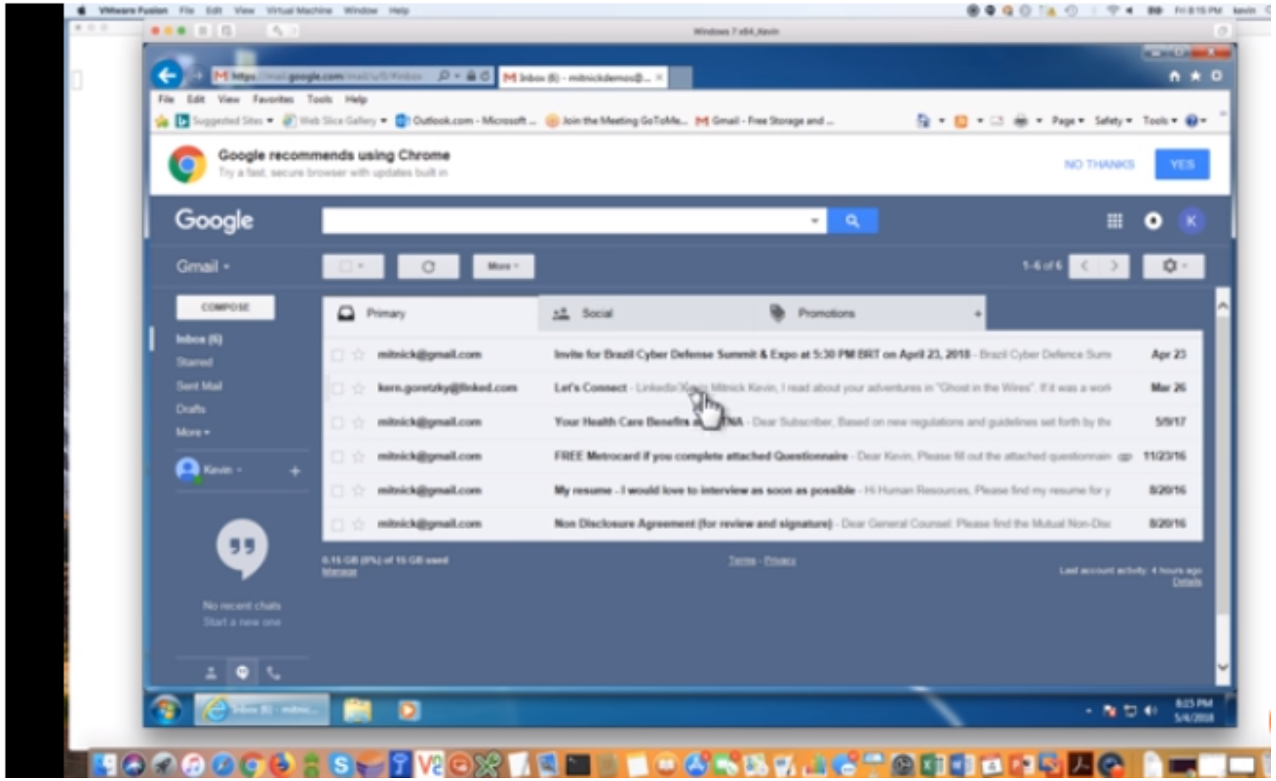
Network Session Hijacking Proxy Theft

1. Bad guy convinces person to visit rogue (usually name-alike) web site, which proxies input to real web site
2. Prompts user to put in MFA credentials
3. User puts in credentials, which bad guy relays to real web site
4. Bad guy logs into real site, and drops legitimate user
5. Takes control over user's account
6. Changes anything user could use to take back control

MFA Hacks

Network Session Hijacking

Kevin Mitnick Hack Demo


Inbox (6) - mitnickdemos@...
File Edit View Favorites Tools Help
Google recommends using Chrome
Try a fast, secure browser with updates built in
NO THANKS
YES
Google
Gmail
More
1-6 of 6
COMPOSE
Inbox (6)
Starred
Sent Mail
Drafts
More
Kevin
Primary
Social
Promotions
No recent chats
Start a new one

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 a[illegible]NA - 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 questionnain 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

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

MFA Hacks

Network Session Hijacking

Kevin Mitnick Hack Demo

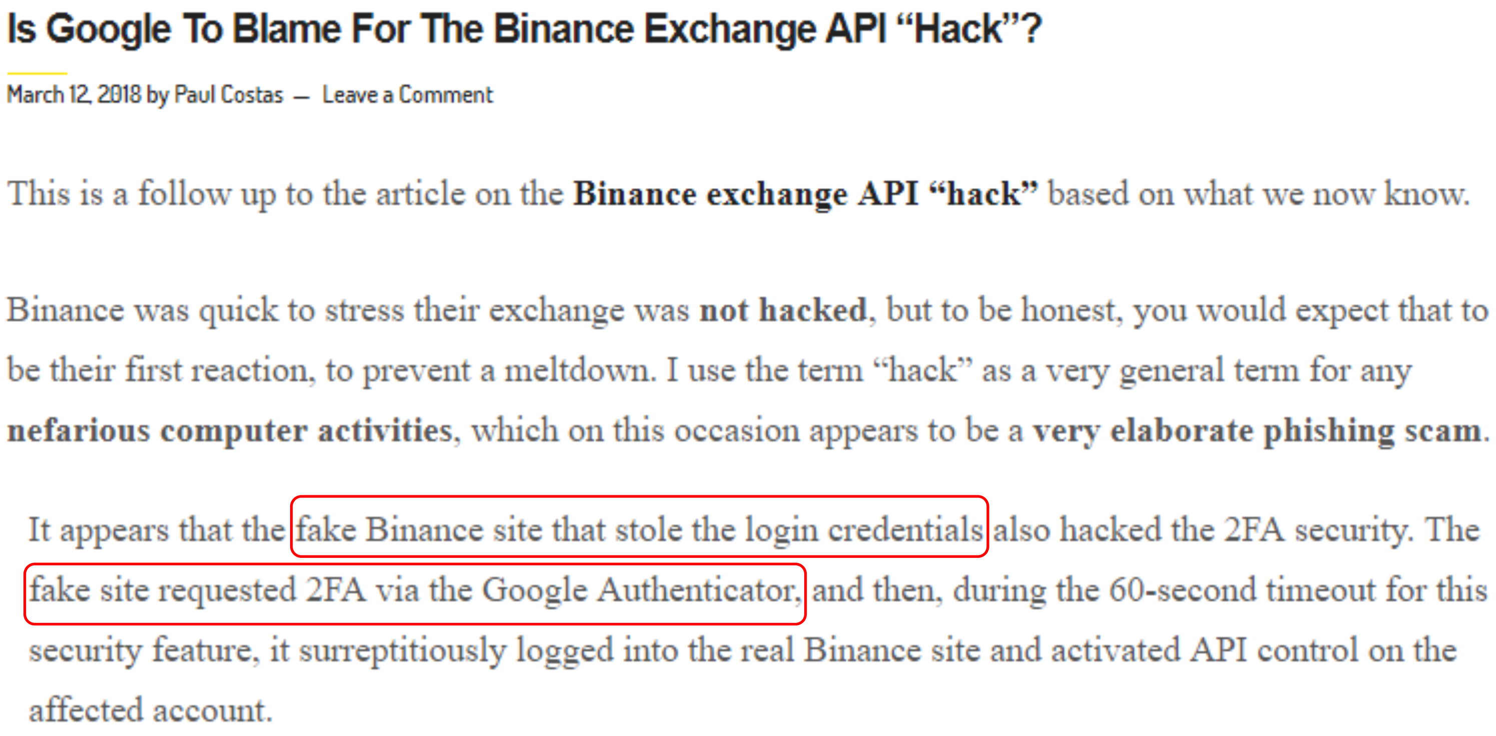
1. Kevin set up fake look-alike/sound-alike web site that was really an evil proxy
2. Tricked user into visiting evil proxy web site
3. User typed in credentials, which proxy, now pretending to be the legitimate customer, presented to legitimate web site
4. Legitimate web site sent back legitimate session 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.

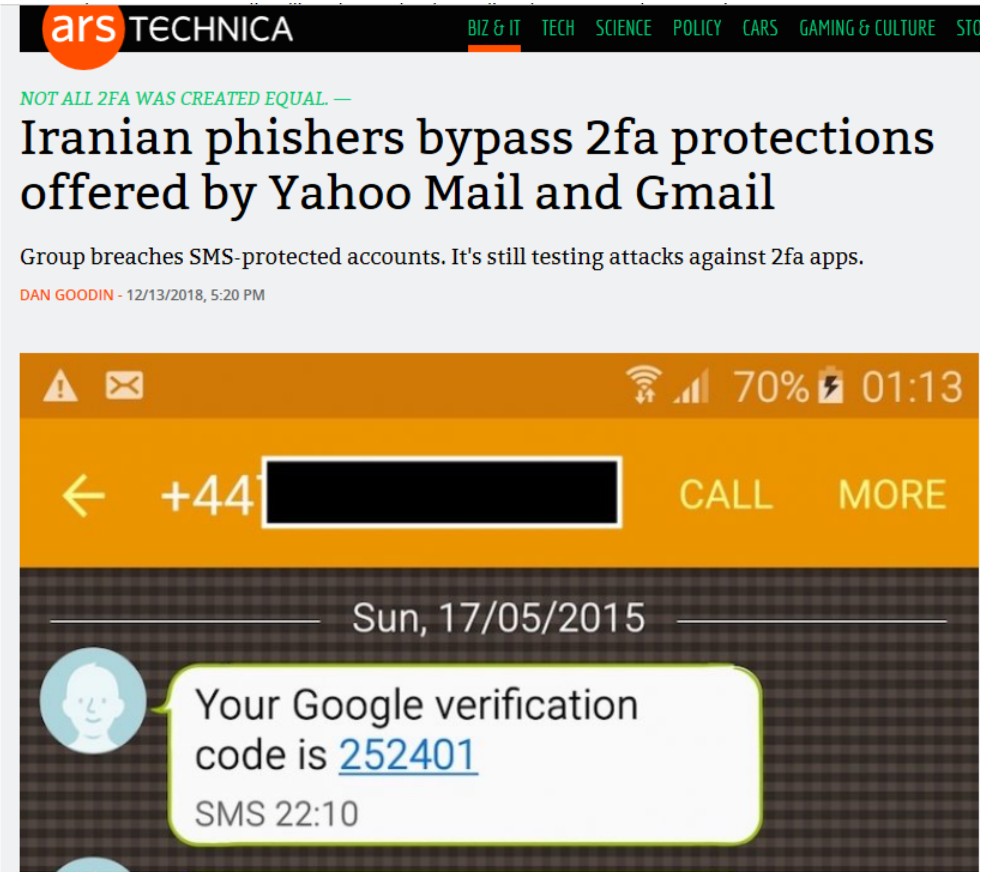
Binance was quick to stress their exchange was **not hacked**, but to be honest, you would expect that to be their first reaction, to prevent a meltdown. I use the term "hack" as a very general term for any **nefarious computer activities**, which on this occasion appears to be a **very elaborate phishing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

Sun, 17/05/2015

Your Google verification code is 252401

SMS 22:10

https://newsroom.mastercard.com/2018/01/17/dispelling-the-myths-the-reality-about-contactless-security-2

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

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

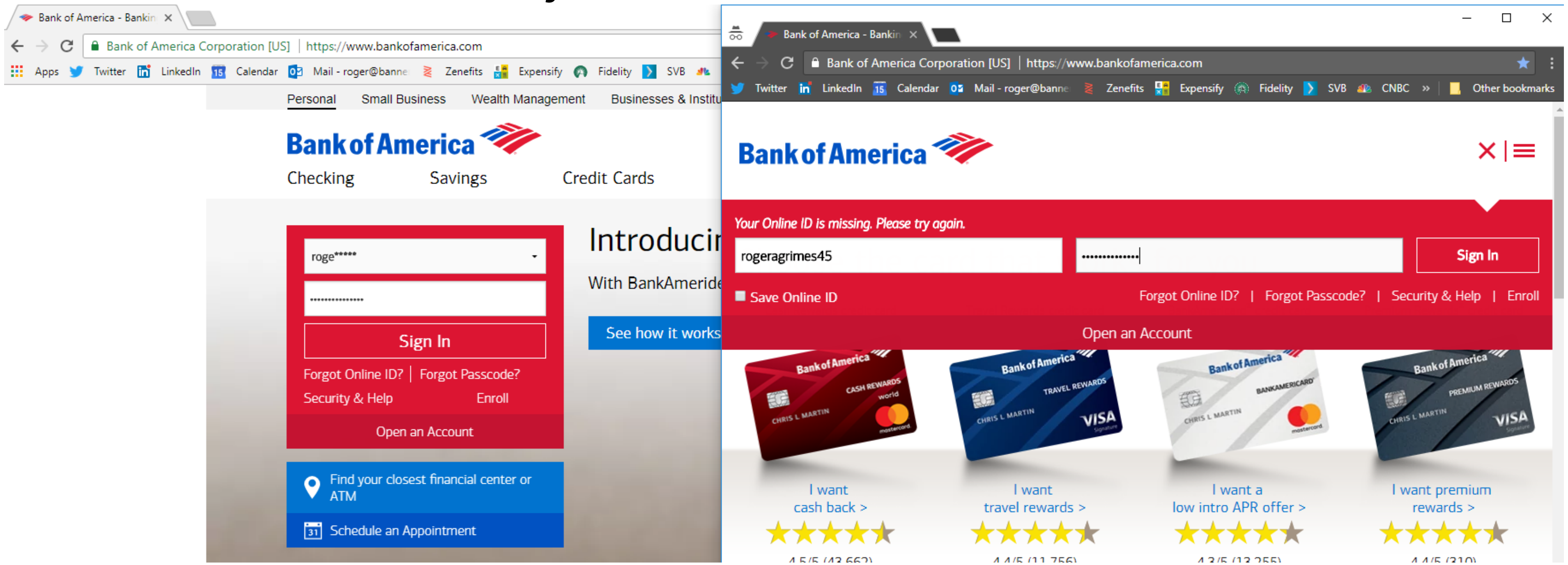
- Attacker can just do everything they want that the user is allowed to do after successful authentication
- Start a second hidden browser session
- Directly steal session cookies
- Insert backdoors
- Invalidate protection all together

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

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



roge*****

Introducir

With BankAmeride

Your Online ID is missing. Please try again.

rogeragrimes45

I want cash back >

4.5/5 (43,662)

I want travel rewards >

4.4/5 (11,756)

I want a low intro APR offer >

4.3/5 (13,255)

I want premium rewards >

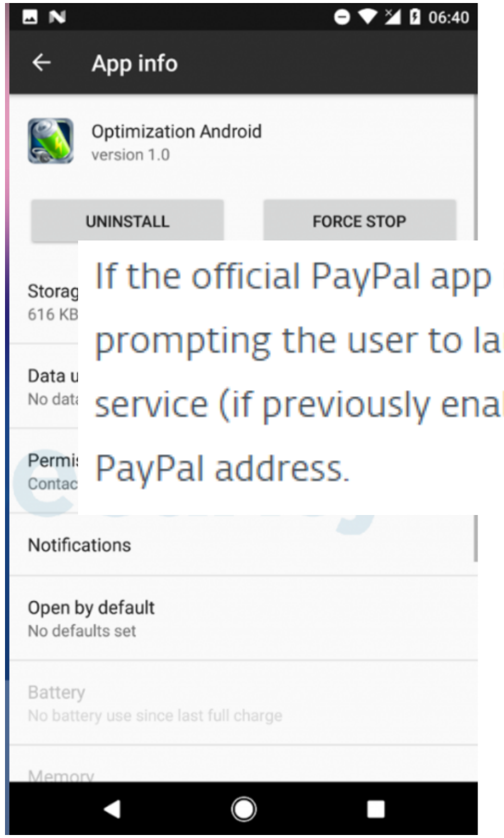
4.4/5 (310)

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

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



06:40

App info

Optimization Android
version 1.0

UNINSTALL

FORCE STOP

Storag
616 KB

Data u
No data

Permis
Contac

Notifications

Open by default
No defaults set

Battery
No battery use since last full charge

Memory

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

Subject Hijack

- Every MFA token or product is uniquely tied to a subject that is supposed to be using the MFA device/software
- If the hacker can take over the subject’s identity within the same namespace, they may be able to reuse the stolen identity with another MFA token/software
- And system will allow a completely unrelated MFA token/software to authenticate and track the fake user as the real user across the system
- Examples:
  - Email hijacking
  - Active Directory/smartcard identity hijacking

MFA Hacks

Subject Hijack Example Summary

Example Attack – Microsoft Smartcard Identity Hijack Scenario Summary

Active Directory integrated smartcards are linked to UPNs

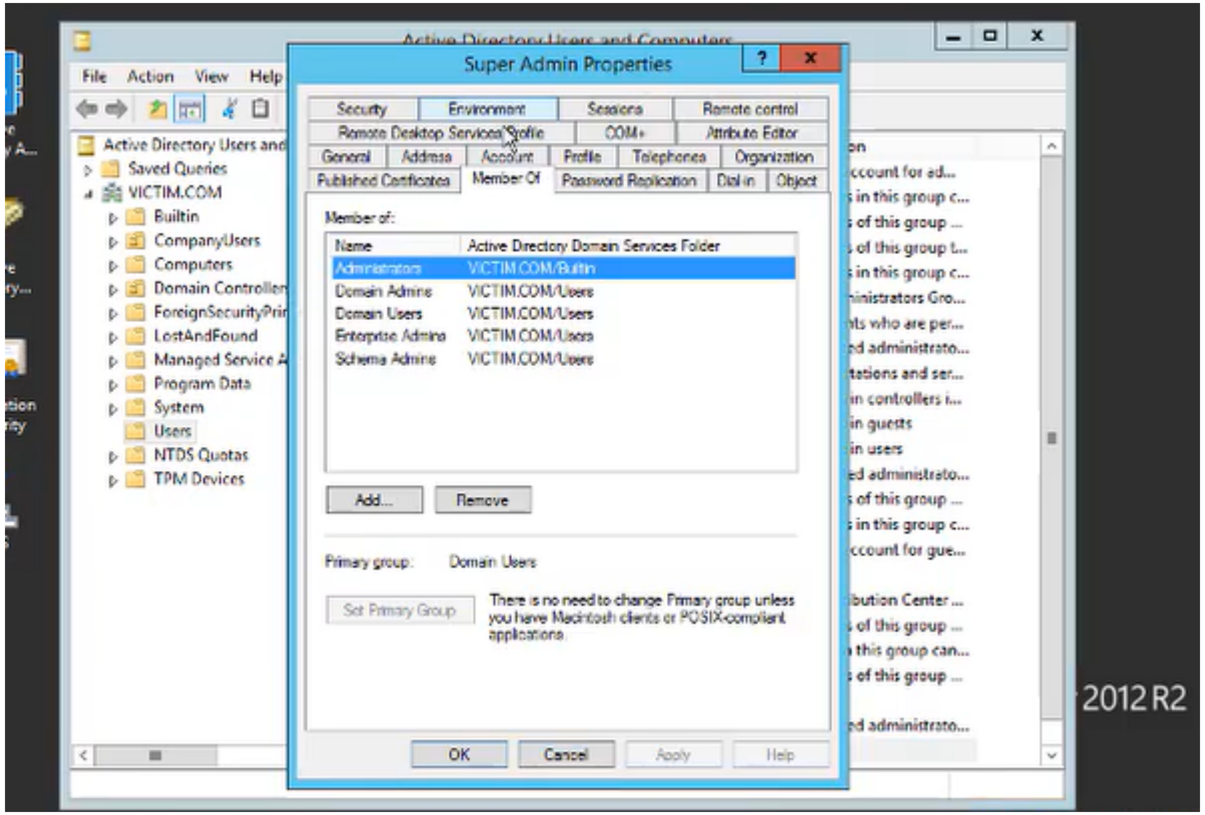
1. Low-privileged HelpDesk admin switches UPNs with SuperAdmin
2. HelpDesk admin logs in using their own HelpDesk smartcard and PIN
3. Viola! HelpDesk admin becomes SuperAdmin, including all group memberships
4. HelpDesk performs malicious actions
5. System tracks all actions as SuperAdmin
6. When HelpDesk is finished, they logout, and switch UPNs back. No one knows the difference

Does your log mgmt. system track and alert on UPN updates?

MFA Hacks

Subject Hijack Example Demo Video

Example Attack – Microsoft Smartcard Identity Hijacking



Member of:

Name	Active Directory Domain Services Folder
Administrators	VICTIM.COM/Builtin
Domain Admins	VICTIM.COM/Users
Domain Users	VICTIM.COM/Users
Enterprise Admins	VICTIM.COM/Users
Schema Admins	VICTIM.COM/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

https://youtu.be/OLQ3lAMuokI

Subject Hacks

Subject Hijack

Defenses

- Realize that any critical attribute (like subject) involved with authentication can be abused
- Review and least privilege permissions on critical attributes
  - For example, UPN in AD allow to change is given to: Enterprise Admins, Domain Admins, Administrators, System, and anyone with Full Control, Write, or Write Public-Information in AD
- Audit and alert on critical attribute changes
- Use MFA systems with 1:1 mappings

MFA Hacks

SIM Swapping

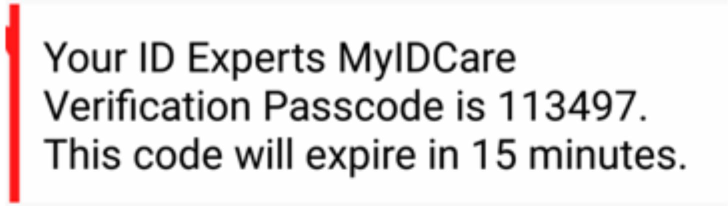
SIM Basics

- 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

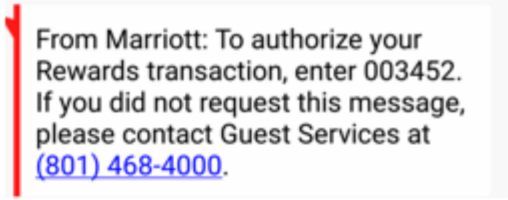
MFA Hacks

SMS-based MFA

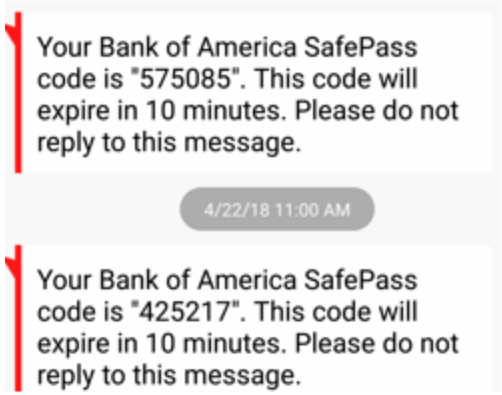
- Many MFA methods included sending additional authentication code via a user’s cell phone short message service (SMS)



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



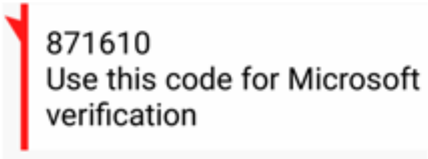
From Marriott: To authorize your Rewards transaction, enter 003452. If you did not request this message, please contact Guest Services at (801) 468-4000.



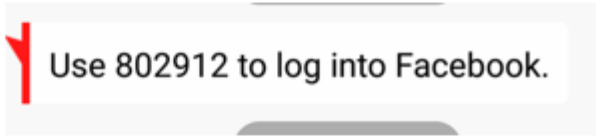
Your Bank of America SafePass code is "575085". This code will expire in 10 minutes. Please do not reply to this message.

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.



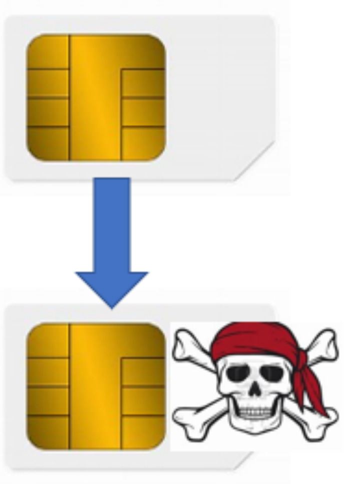
871610
Use this code for Microsoft verification



Use 802912 to log into Facebook.

MFA Hacks

SIM Swapping Attacks

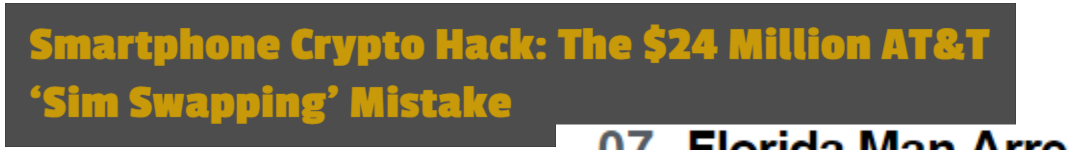


- In a SIM swapping attack, the attacker transfers the victim's SIM information to another phone, allowing the attacker to get the any sent codes used by SMS-based MFA solutions
  - Old phone "silently" stops working
- Usually done by hack social engineering cell phone vendor's support techs; or using 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

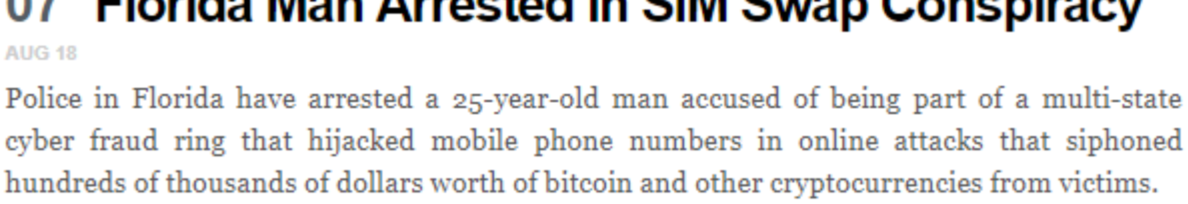
MFA Hacks

SIM Swapping Attacks

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



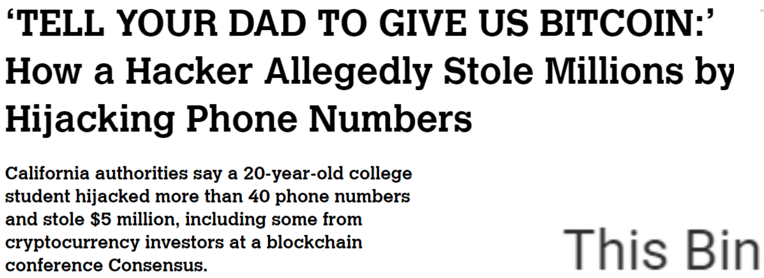
Smartphone Crypto Hack: The $24 Million AT&T 'Sim Swapping' Mistake



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

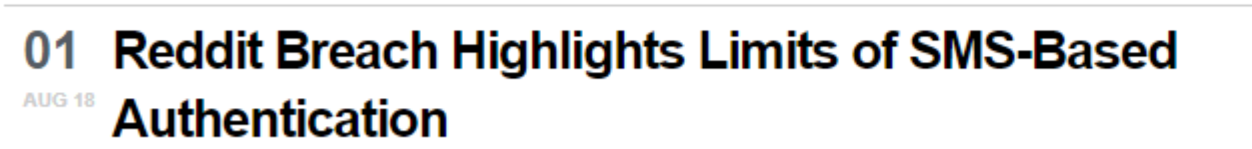
AUG 18

Police in Florida have arrested a 25-year-old man accused of being part of a multi-state cyber fraud ring that hijacked mobile phone numbers in online attacks that siphoned hundreds of thousands of dollars worth of bitcoin and other cryptocurrencies from victims.



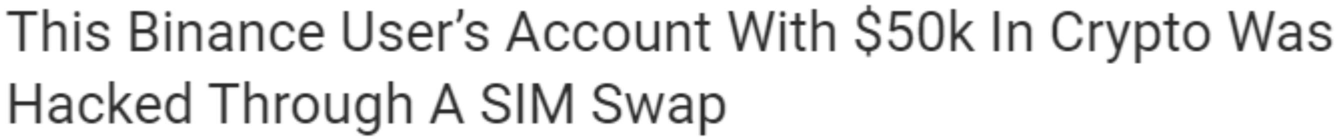
'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers

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.

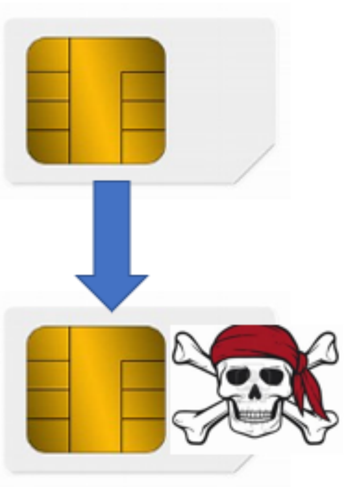


01 **Reddit Breach Highlights Limits of SMS-Based Authentication**

AUG 18



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



MFA Hacks

SIM Swapping

SIM 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 SIM-swapping attacks

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

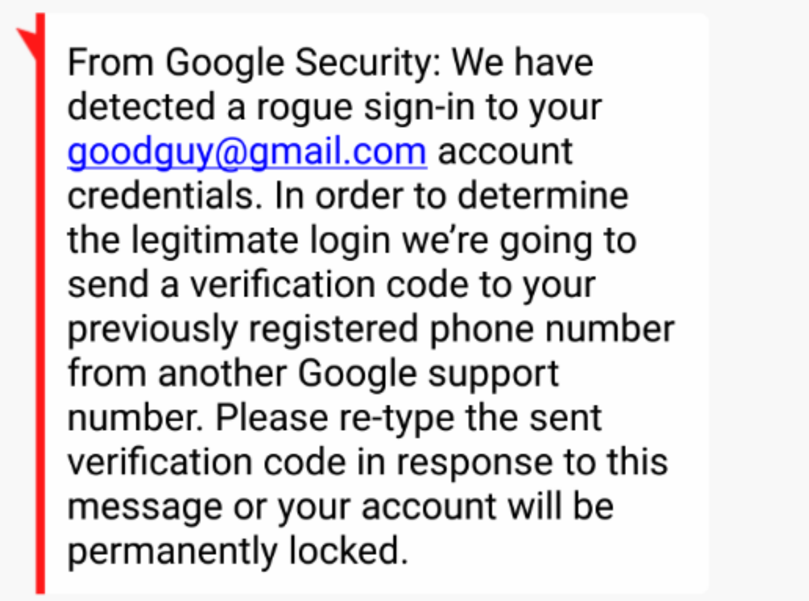
Rogue Recoveries

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.

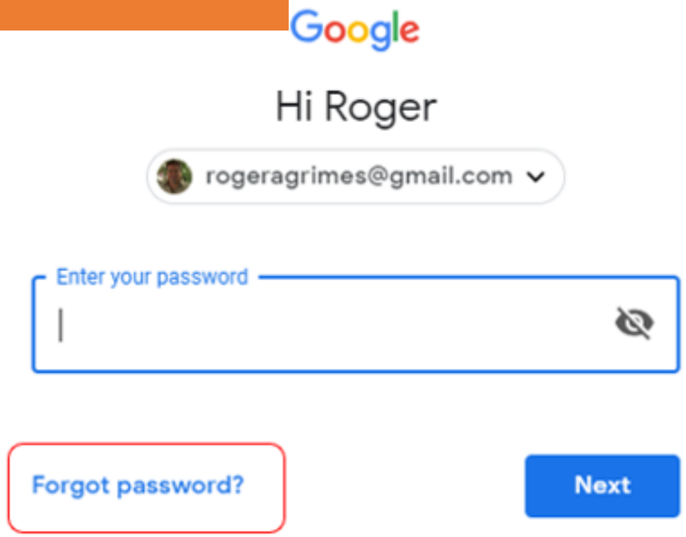
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

2. Hacker forces your email account into SMS PIN recovery

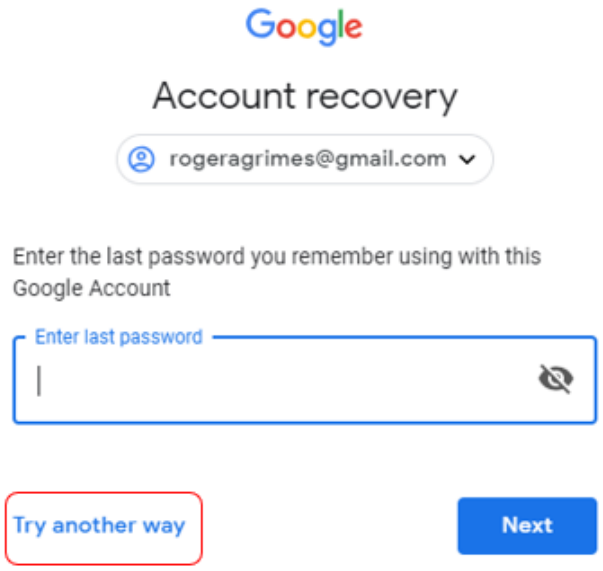


Google

Hi Roger

rogeragrimes@gmail.com

Enter your password



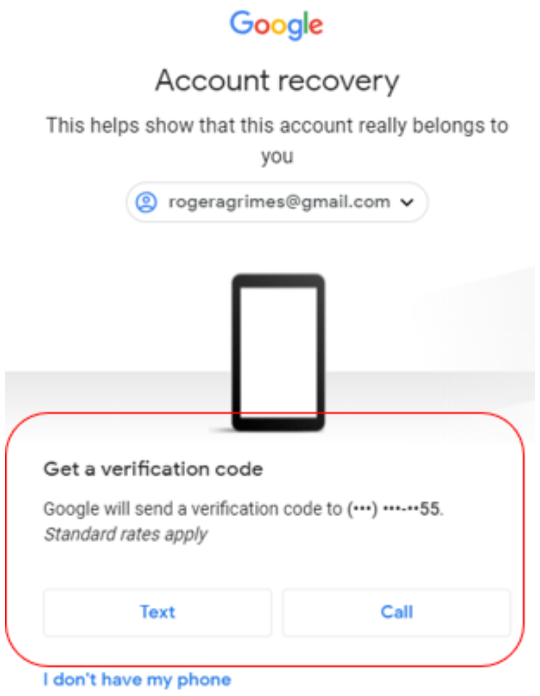
Google

Account recovery

rogeragrimes@gmail.com

Enter the last password you remember using with this Google Account

Enter last password



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

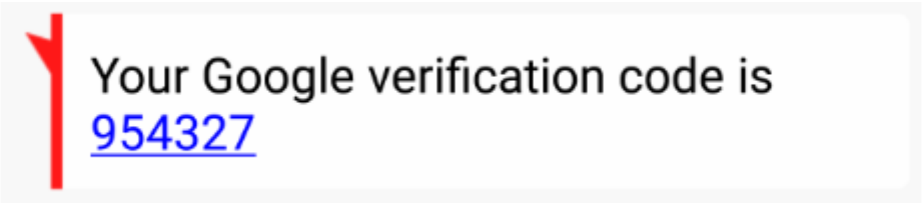
Rogue Recoveries

SMS Rogue Recovery

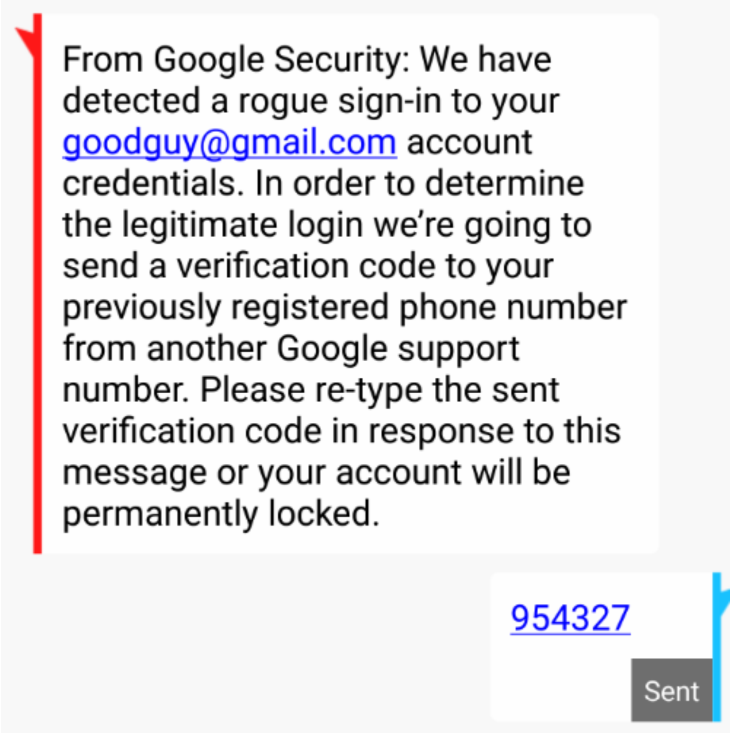
Hacking Into Your Email Using Recovery Methods

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

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

4. Hacker uses your SMS PIN code to login to your email account and take it over

Note: To be fair, Google has some of the best recovery options of any email provider, including that it can send a non-SMS message to your phone before the hacker can even get to the SMS code screen to get Google to send an SMS message

Rogue Recoveries

SMS Rogue Recovery

Defenses

- Be aware of rogue recovery messages
- Recognize when SMS recovery PINs should be typed into browsers, not (usually) back into SMS
- Use MFA when possible
- Try to avoid alternate email-based recovery methods
- Try to avoid SMS-based recovery based methods
- Try to minimize public posting of phone numbers related to your recovery account methods

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

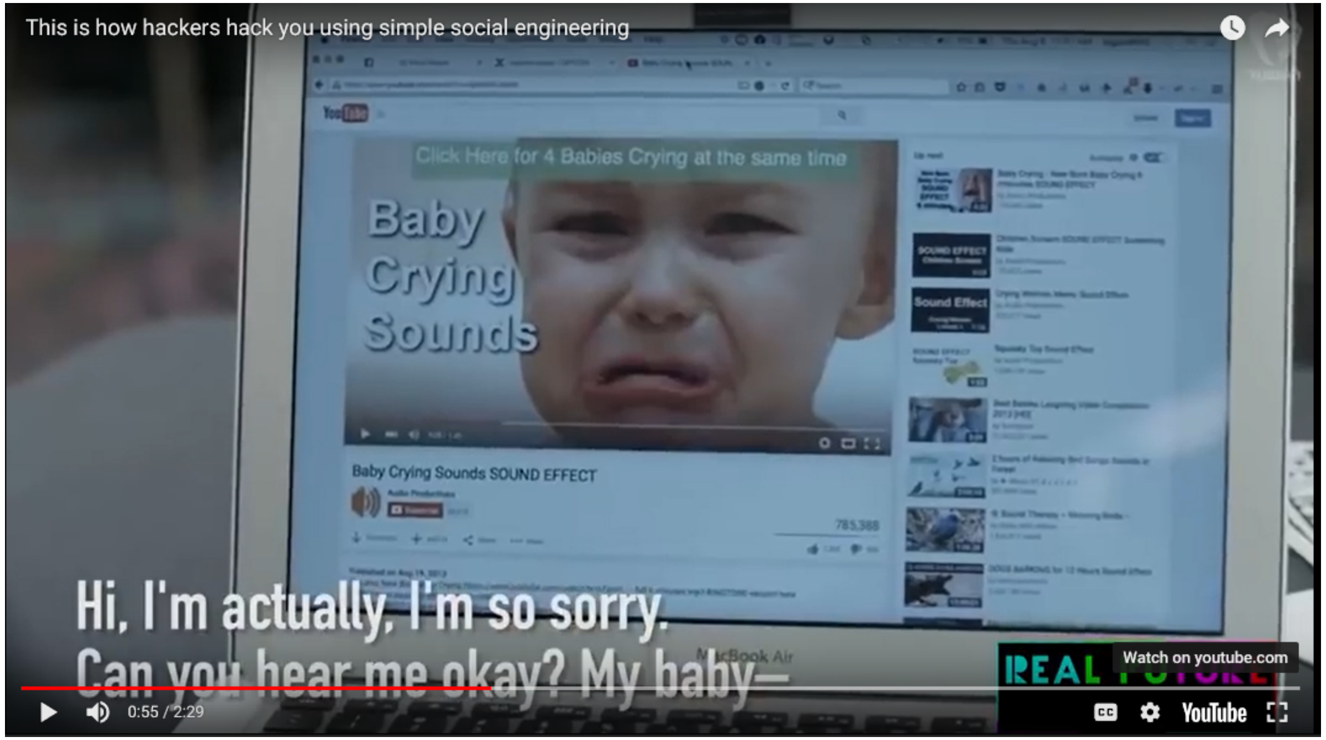
MFA Hacks

Social Engineer Tech Support

Great Example

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

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



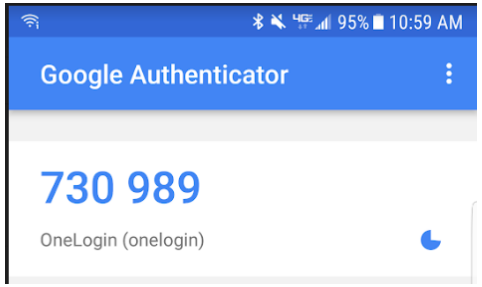
This is how hackers hack you using simple social engineering

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

Click Here for 4 Babies Crying at the same time
Baby Crying Sounds
Baby Crying Sounds SOUND EFFECT
0:55 / 2:29
Watch on youtube.com
YouTube
REAL FUTURE

MFA Hacks

Duplicate Code Generator



730 989

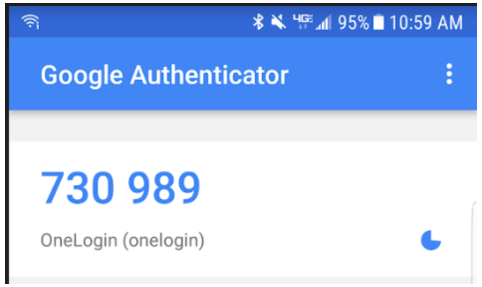
OneLogin (onelogin)

- 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



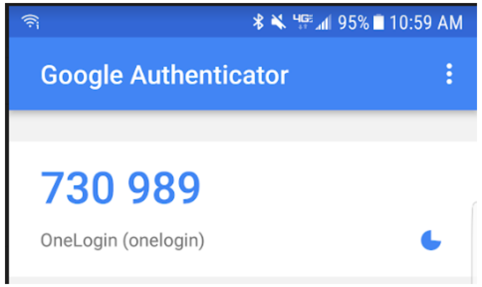
730 989

OneLogin (onelogin)

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

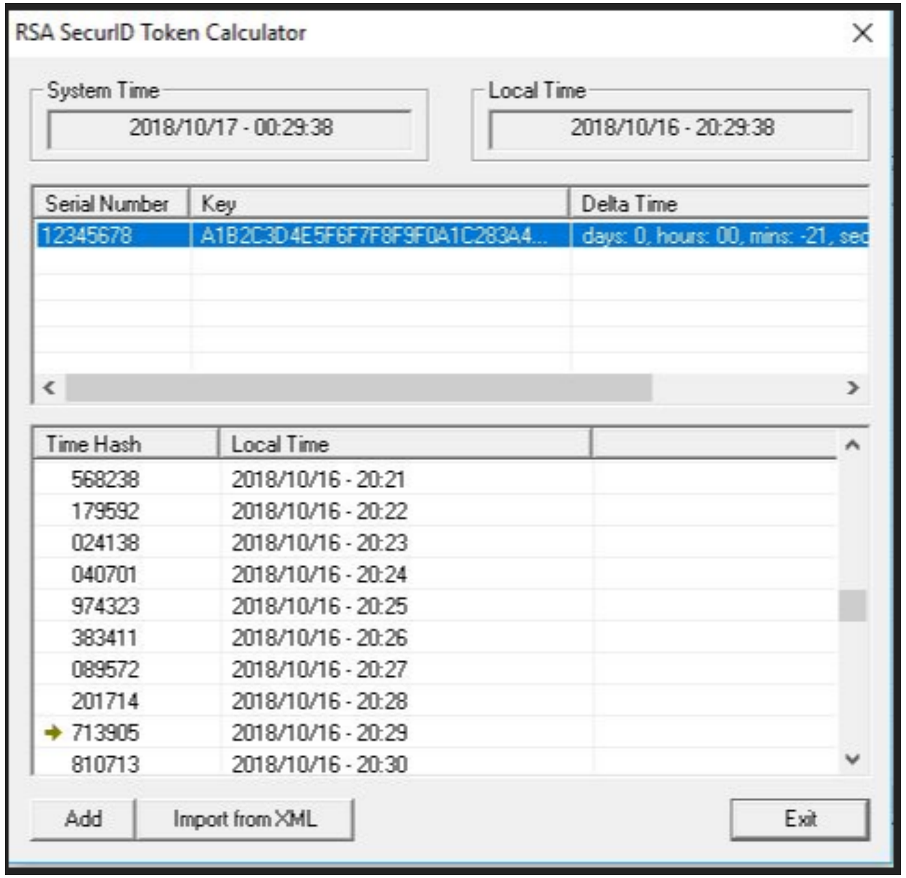
MFA Hacks

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

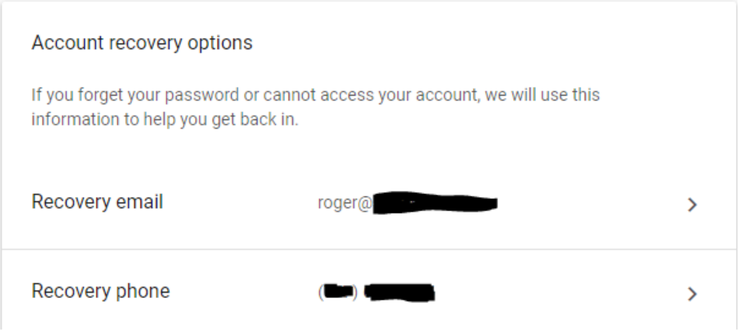
Not Required/ Downgrade Attacks

- 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

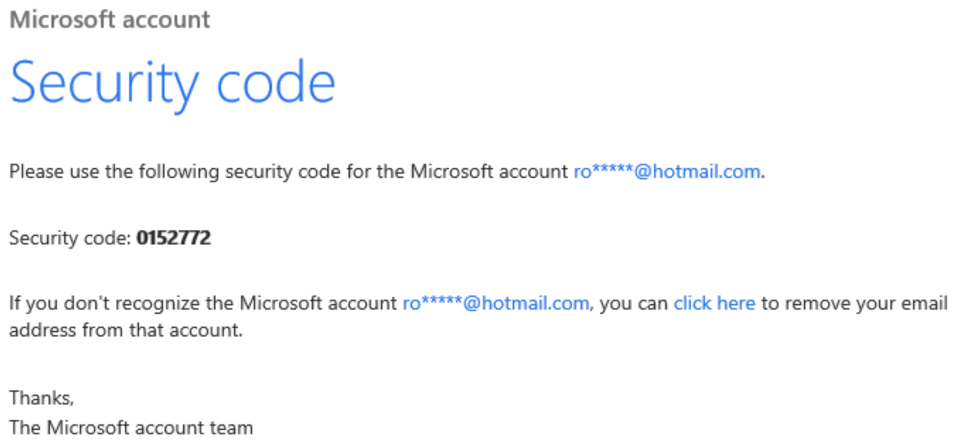


Account recovery options

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] ›



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.

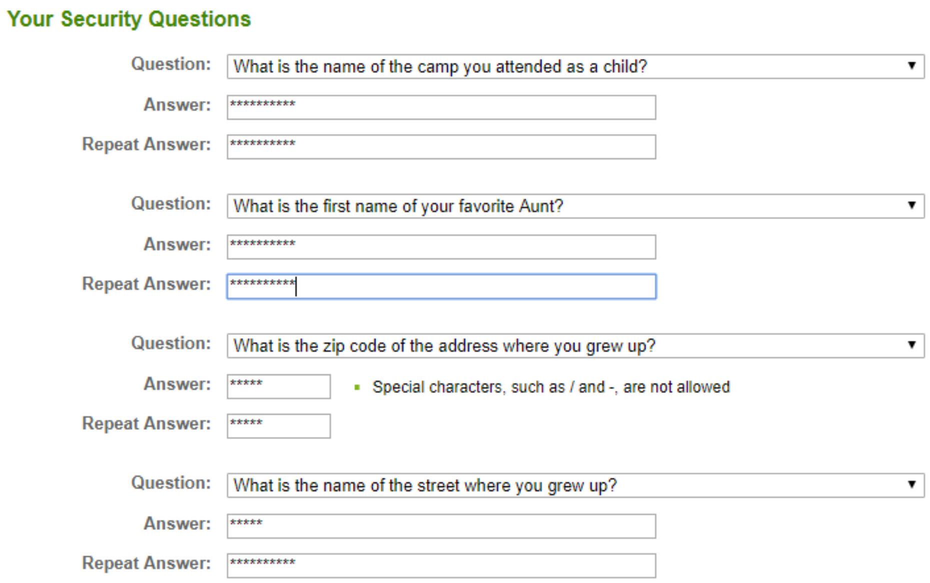
Thanks,
The Microsoft account team

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

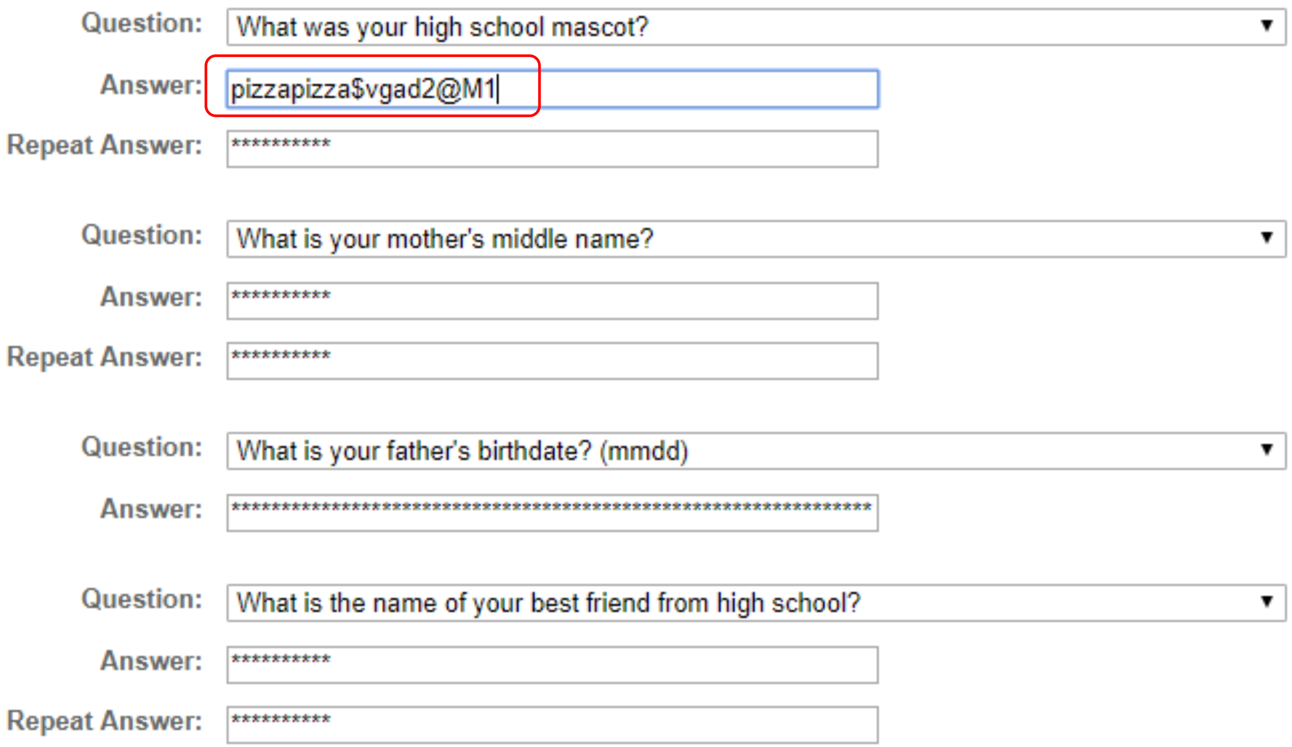
Problem: Answers can often be easily guessed by hackers

- 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

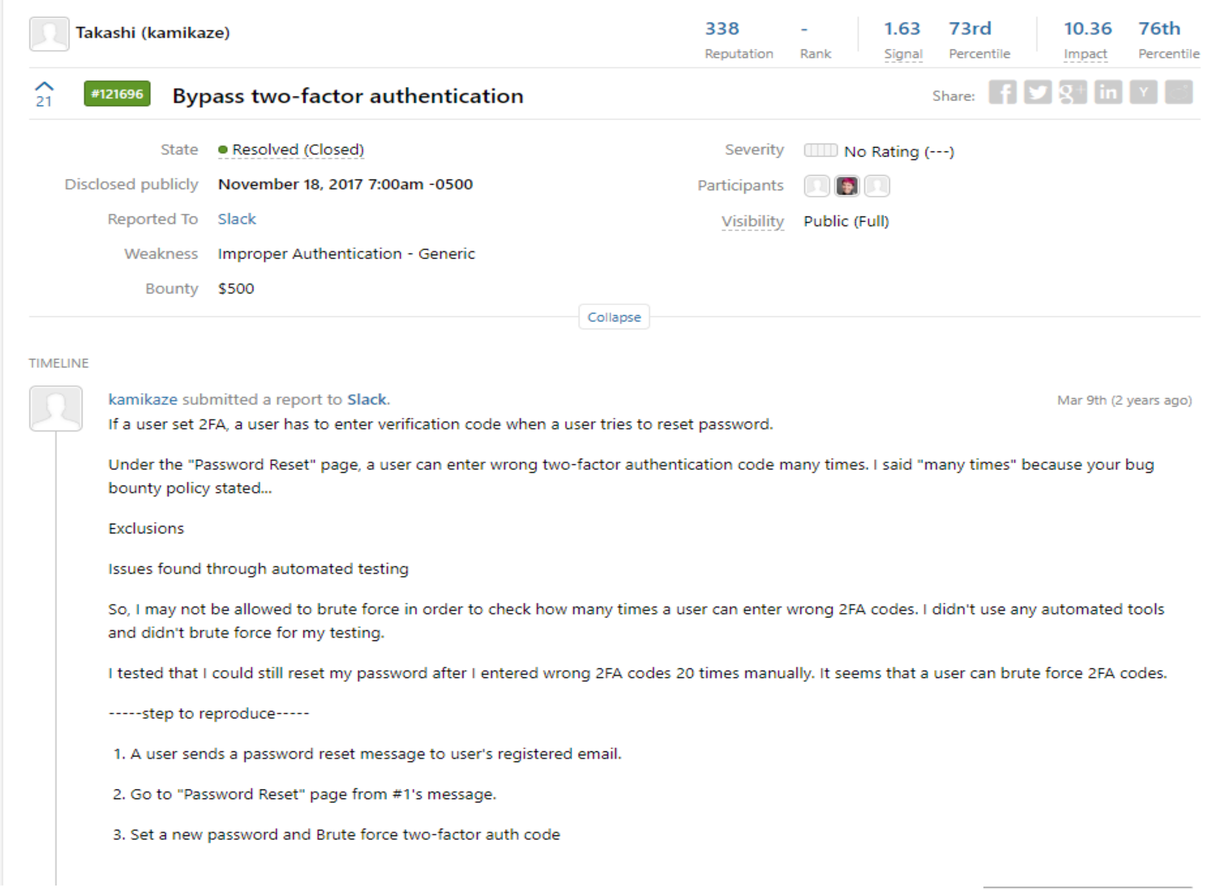
Hijacking Shared Auth & APIs

- It’s very possible for shared authentication schemes, like oAuth, to have session tokens stolen and reused
- When you successfully authenticate to one web site that supports integrate auth, you are essentially allowing hacker into any other web site that supports the same integrated auth method for your identity
- So even if the next web site requires MFA, the integrated auth will usually seamlessly authenticate the person, bypassing the MFA, using the previous shared master session token
- Has been used by many APT attacks in the past
  - https://www.securityweek.com/google-tightens-oauth-rules-combat-phishing

MFA Hacks

Brute Force

- If the MFA auth screen doesn’t include account lockouts for x number of bad attempts, hackers can brute force their way into it
- Happens all the time



Takashi (kamikaze)

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

21 #121696 Bypass two-factor authentication

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		

TIMELINE

kamikaze submitted a report to Slack. Mar 9th (2 years ago)

If a user set 2FA, a user has to enter verification code when a user tries to reset password.

Under the "Password Reset" page, a user can enter wrong two-factor authentication code many times. I said "many times" because your bug bounty policy stated...

Exclusions

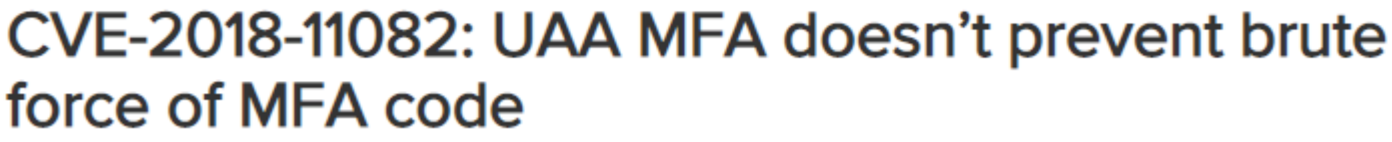
Issues found through automated testing

So, I may not be allowed to brute force in order to check how many times a user can enter wrong 2FA codes. I didn't use any automated tools and didn't brute force for my testing.

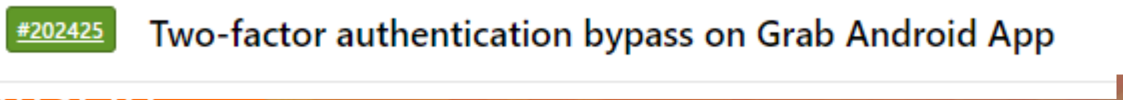
I tested that I could still reset my password after I entered wrong 2FA codes 20 times manually. It seems that a user can brute force 2FA codes.

-----step to reproduce-----

1. A user sends a password reset message to user's registered email.
2. Go to "Password Reset" page from #1's message.
3. Set a new password and Brute force two-factor auth code



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

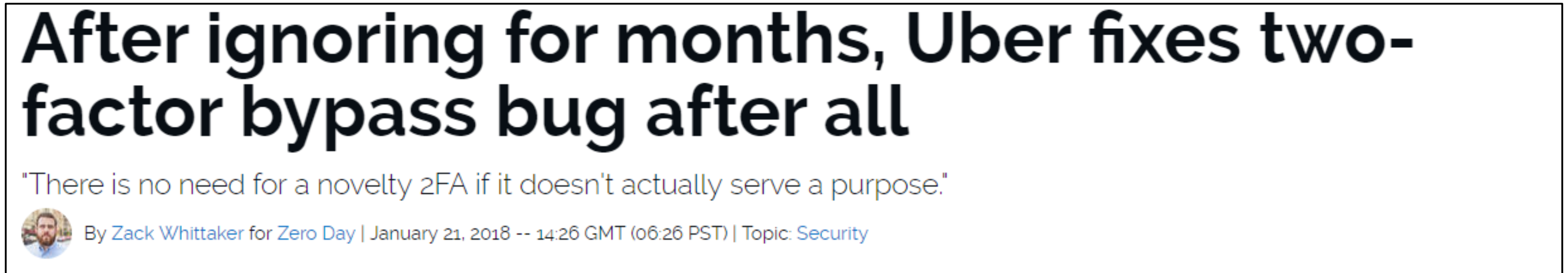


#202425 Two-factor authentication bypass on Grab Android App

MFA Hacks

Buggy MFA

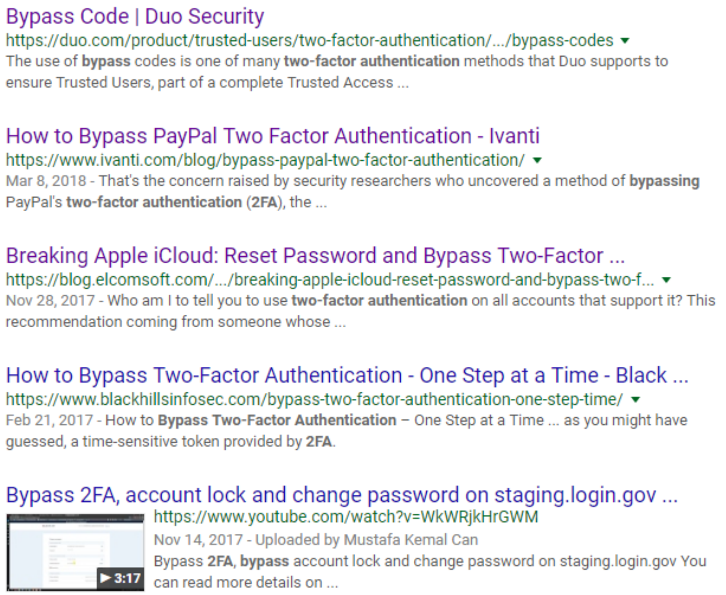
- Bugs are bugs, some bypass MFA



After ignoring for months, Uber 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 ...
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

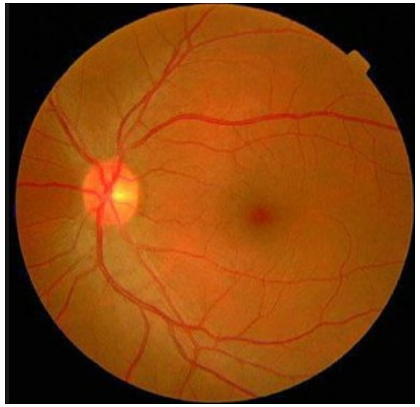
- Sometimes a single bug impacts hundreds of millions of otherwise unrelated MFA devices
- Huge bug making any MFA product (smartcards, TPM chips, Yubikeys, etc.) with Infineon-generated RSA key lengths of 2048 or smaller (which is most of them), easy to extract the PRIVATE key from public key.
- Still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

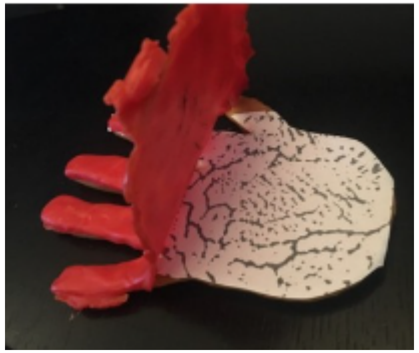
MFA Hacks

Physical Attacks

Biometric

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



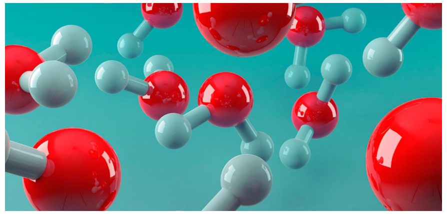


MFA Hacks

Physical Attacks

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

Defending Against MFA Attacks

Defending Against MFA Attacks

Defenses

Social Defenses

- Education – for admins and end-users
- Realize nothing is unhackable
- Include MFA hacking awareness into your security awareness training
  - Share this slide deck with co-workers and mgmt.
- Don’t get tricked into clicking on rogue links
- Block rogue links as much as possible
- Make sure URL is legitimate

Defending Against MFA Attacks

Defenses

Technical Defenses

- Enable REQUIRED MFA whenever possible
- Don’t use SMS-based MFA whenever possible
- Use “1:1” MFA solutions, which require client-side to be pre-registered with server
- Use/require 2-way, mutual, authentication whenever possible
  - Ex. FIDO U2F’s Channel or Token Binding
- Does your MFA solution specifically fight session token theft and/or malicious replays (i.e. replay resistant)
- Can your MFA vendor’s support help be socially engineered?
- Make sure MFA vendors use secure development lifecycle (SDL) in their programming
- Make sure MFA has “bad attempt throttling” or “account lockout” enabled

Defending Against MFA Attacks

Defenses

Technical Defenses (con’t)

- Spread factors across different “channels” or “bands” (in-band/out-band)
- Protect and audit identity attributes used by MFA for unique identification of MFA logons
- Don’t answer password reset questions using the honest answers.
- Encourage and use sites and services to use dynamic authentication, where additional factors are requested for higher risk circumstances
- Understand the risks of “shared secret” systems
- For transaction-based authentication, need to send user all critical details out-of-band before confirmation is transmitted/required

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
- If you use or consider going to MFA, security awareness training has still got to be a big part of your overall security defense

For More Information

Read More

- Applied Cryptography Group
  - https://crypto.stanford.edu/
- Quest to Replace Passwords whitepaper
  - https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/QuestToReplacePasswords.pdf
- Joseph Bonneau
  - http://jbonneau.com/
- NIST Digital Identity Guides
  - https://pages.nist.gov/800-63-3/
- Check to see if a web site supports MFA
  - https://twofactorauth.org/
- FIDO Alliance
  - https://fidoalliance.org/

Resources

Free IT Security Tools

Domain Doppelgänger

Awareness Program Builder

Domain Spoof Tool

Mailserver Security Assessment

Phish Alert

Ransomware Simulator

Weak Password Test

Phishing Security Test

Second Chance

Email Exposure Check Pro

Training Preview

Breached Password Test

KnowBe4

Password:

****

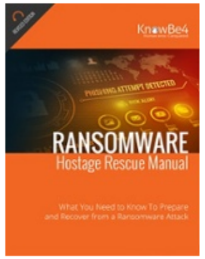
WHITE PAPER

12+ Ways to Hack Two-Factor Authentication

12+ Ways to Hack Two-Factor

All multi-factor authentication (MFA) mechanisms can know how to defend against MFA hacks? This whitepa those attacks.

Whitepapers



KnowBe4

RANSOMWARE

Hostage Rescue Manual

What You Need to Know To Prepare and Recover from a Ransomware Attack

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

KnowBe4

CEO FRAUD

Prevention Manual

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

» Learn More at www.KnowBe4.com/Resources «

Questions?

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