RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: IDY-F02

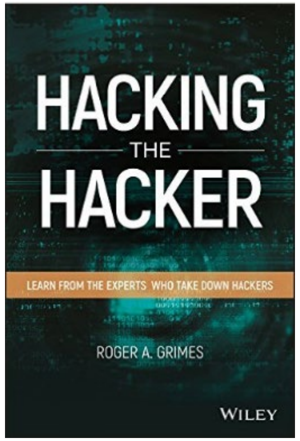
12 Ways to Hack MFA

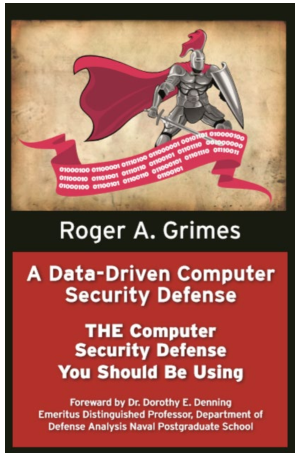
Roger A. Grimes

Data-Driven Defense Evangelist
KnowBe4, Inc.
@rogeragrimes

About Roger

- Data-Driven Defense Evangelist for KnowBe4, Inc.
- 30-years plus in computer security
- Expertise in host and network security, IdM, crypto, APT, honeypots, 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




Roger A. Grimes
A Data-Driven Computer Security Defense
THE Computer Security Defense You Should Be Using
Foreword by Dr. Dorothy E. Denning
Emeritus Distinguished Professor, Department of Defense Analysis Naval Postgraduate School

Certifications passed include:

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

KnowBe4
Human error. Conquered.

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
- Location, behavior, 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
  - With MFA, client is usually proving identity to server
    - But because server is not authenticated, rogue servers can be involved
- **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 and 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)

RSAConference2019

Hacking MFA

MFA Hacks

General

Main Hacking Methods

- **Social Engineering**
- **Technical Attack** against underlying technology

- Some of the attacks are both
- 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

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

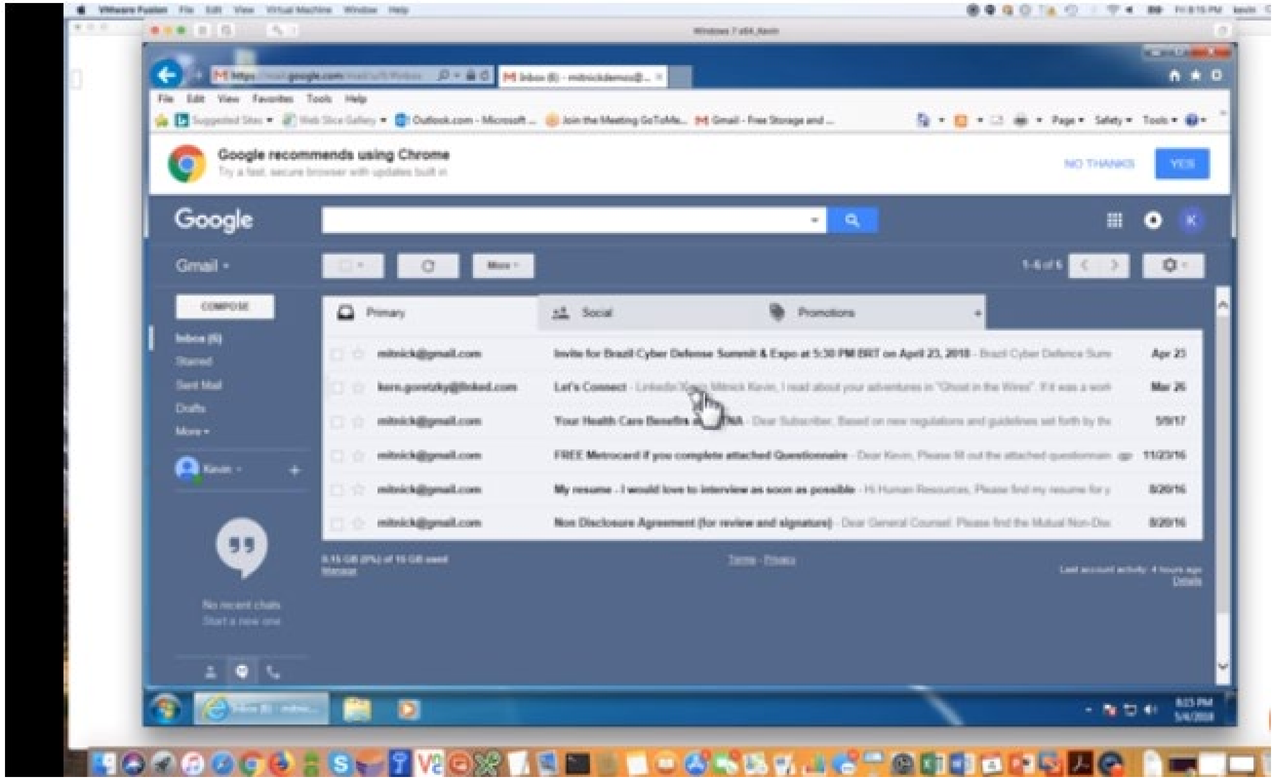
Network Session Hijacking Proxy Theft

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



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... 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 questionnaire	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

0.15 GB (0%) of 15 GB used
Manage

Terms - Privacy

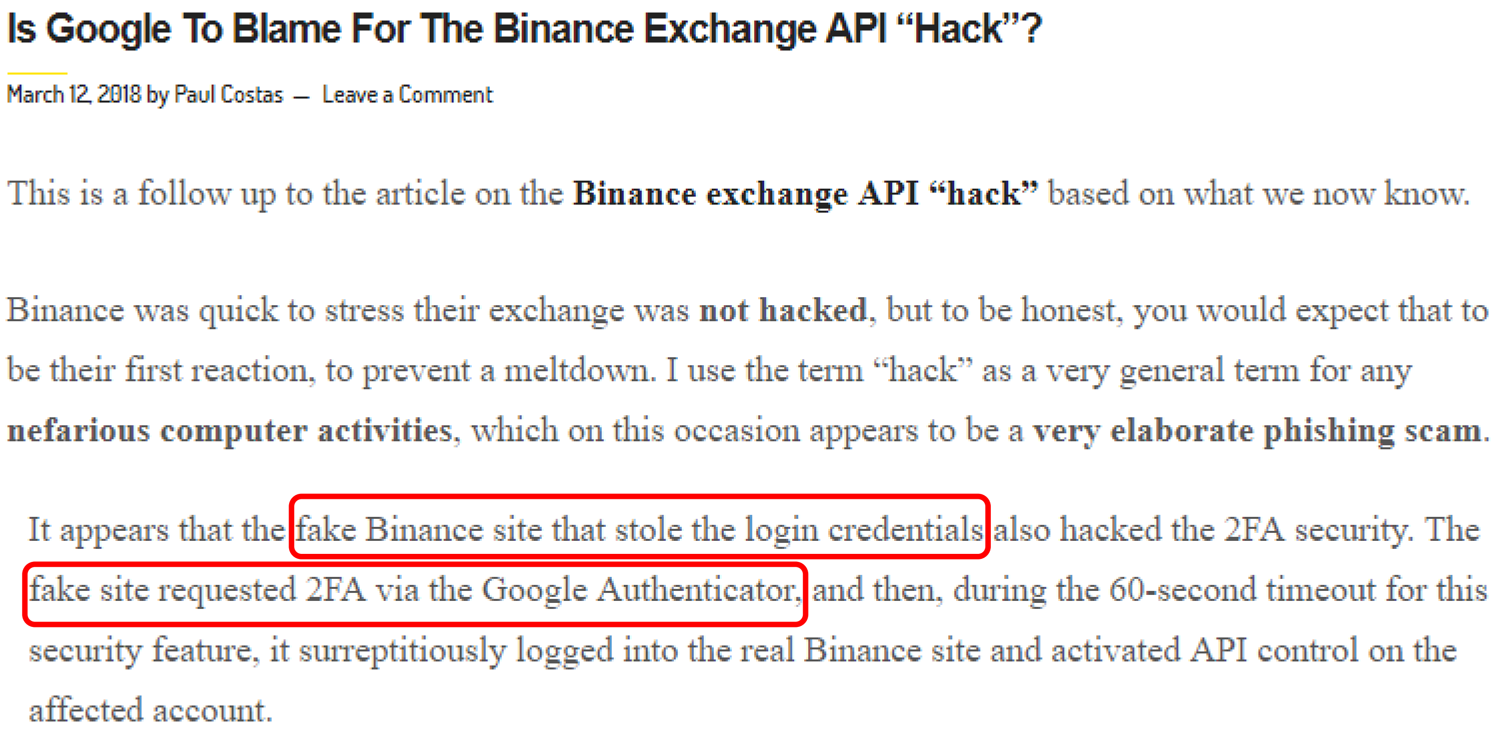
Last account activity: 4 hours ago
Details

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

MFA Hacks

Network Session Hijacking

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.

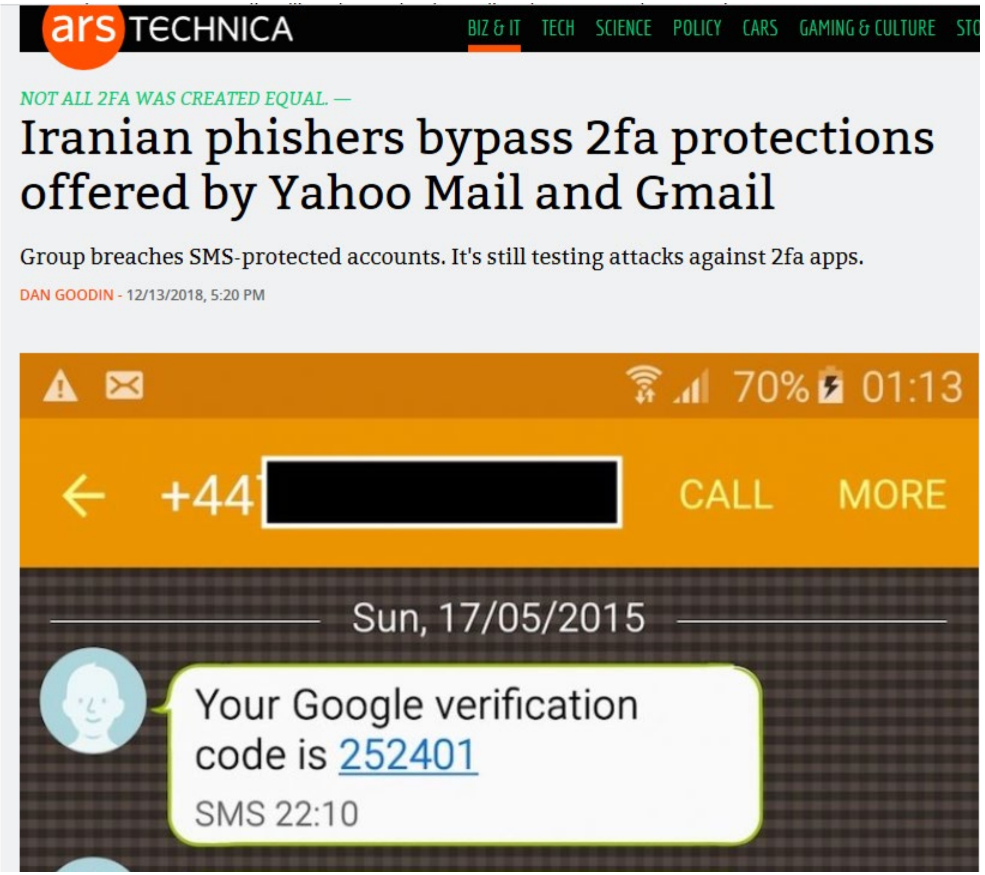
Binance was quick to stress their exchange was **not hacked**, but to be honest, you would expect that to be their first reaction, to prevent a meltdown. I use the term "hack" as a very general term for any **nefarious computer activities**, which on this occasion appears to be a **very elaborate phishing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

+44[redacted]

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

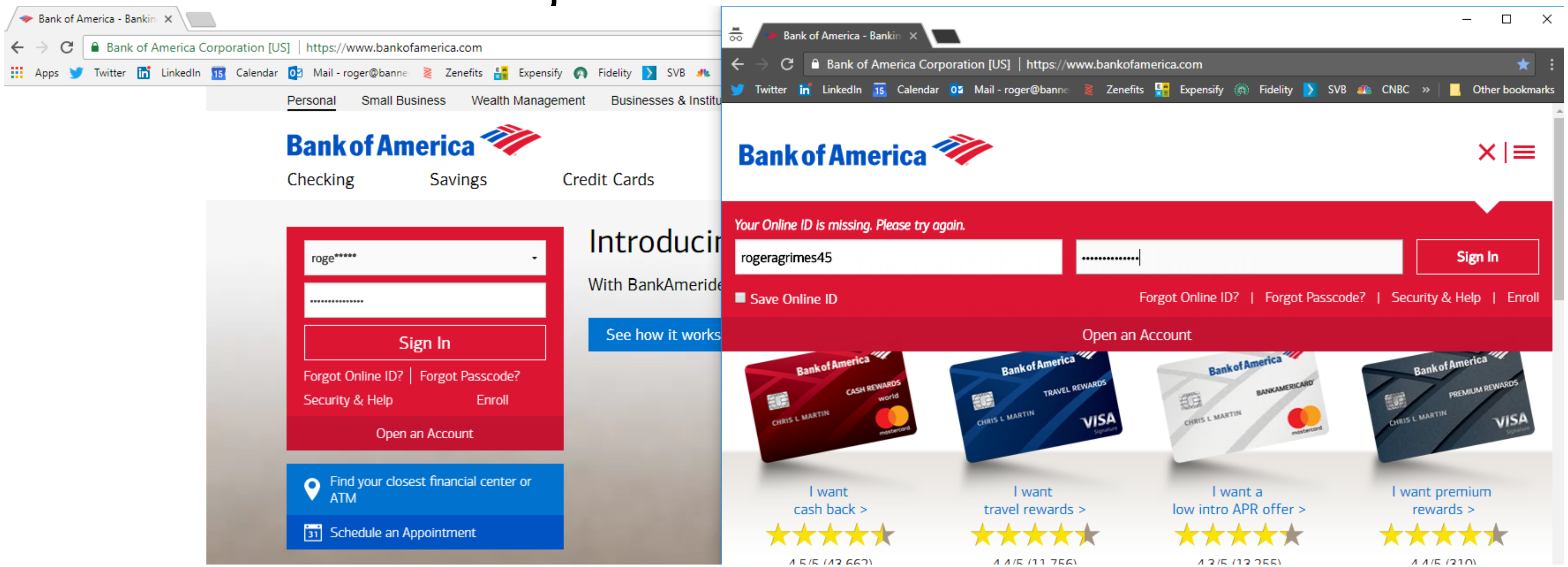
- Attacker can just do everything they want that the user is allowed to do after successful authentication
- Start a second hidden browser session
- Directly steal session cookies
- Insert backdoors
- Invalidate protection all together

MFA Hacks

Endpoint Attacks

Man-in-the-Endpoint Attacks

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


Bank of America - Bankin
Bank of America Corporation [US] | https://www.bankofamerica.com
Apps Twitter LinkedIn Calendar Mail - roger@banne Zenefits Expensify Fidelity SVB CNBC Other bookmarks
Personal
Small Business
Wealth Management
Businesses & Institu
Bank of America
Checking
Savings
Credit Cards
Introducin
With BankAmeride
See how it works
Sign In
Forgot Online ID? | Forgot Passcode?
Security & Help
Enroll
Open an Account
Find your closest financial center or ATM
Schedule an Appointment
Save Online ID
Forgot Online ID? | Forgot Passcode? | Security & Help | Enroll
I want cash back >
I want travel rewards >
I want a low intro APR offer >
I want premium rewards >

roge*****

Your Online ID is missing. Please try again.

rogeragrimes45

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 identifier within the same namespace, they may be able to use stolen identifier 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
  - Smartcard/Active Directory hijacking

MFA Hacks

Subject Hijack Example Summary

Example Attack – Microsoft Smartcard Identifier Hijacking - Summary

Active Directory integrated smartcards are linked to UPNs

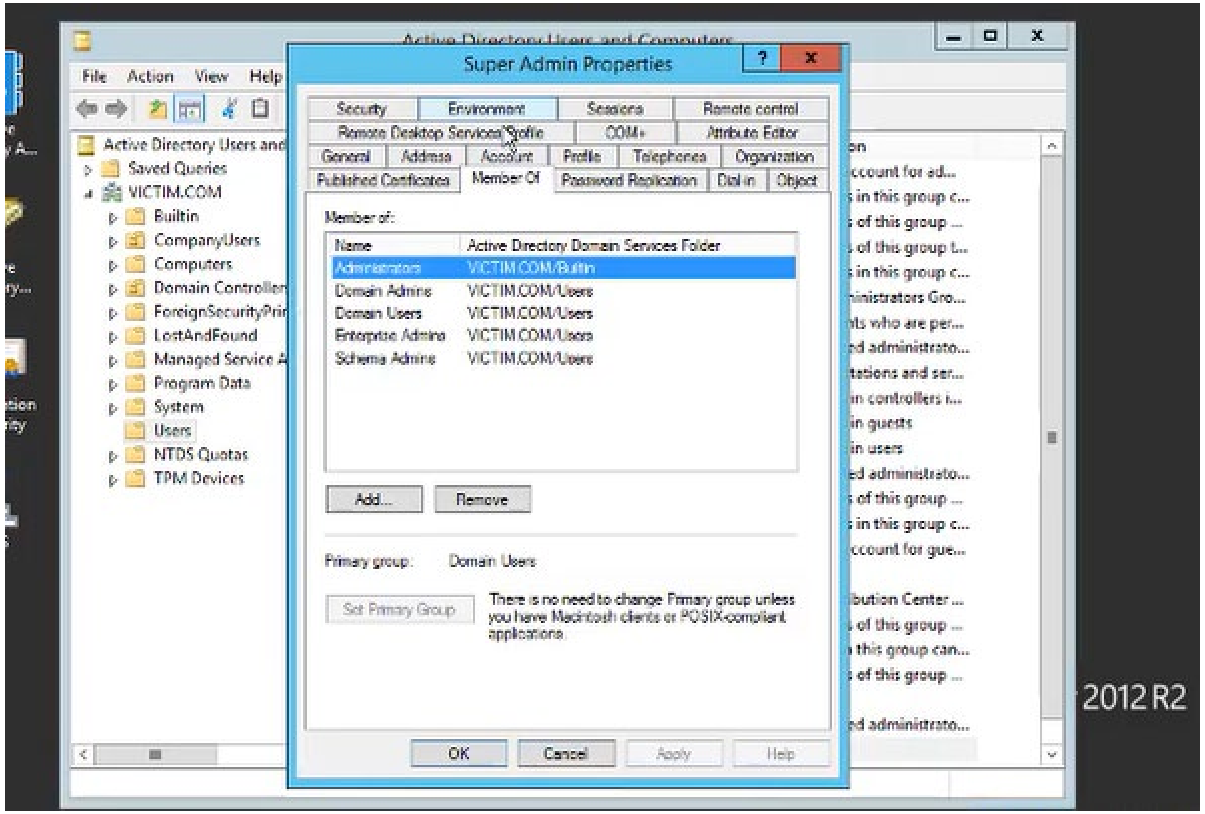
1. Low-privileged HelpDesk admin switches UPNs with SuperAdmin
2. HelpDesk admin logs in using their own HelpDesk smartcard and PIN
3. Viola! HelpDesk admin becomes SuperAdmin, including all group memberships
4. HelpDesk performs malicious actions
5. System tracks all actions as SuperAdmin
6. When HelpDesk 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 Identifier 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

<u>Defenses</u>

- 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

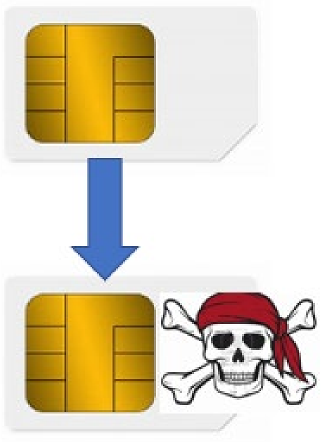
SIM Basics

- SIM stands for **S**ubscriber **I**dentity **M**odule
- Most cell phone SIM cards store the cell phone network's information and the subscriber's (user/owner) information, plus can store app data
- If you move the SIM card (or its info) to another cell phone, it transfers your phone number and other info to that other cell phone
  - Once done, "old" phone stops working

MFA Hacks

SIM Swapping Attacks

- Many, especially early, MFA methods included sending additional authentication code via a user’s cell phone short message service (SMS)
- A SIM swapping attack can steal/transfer the user’s cell phone operations to another phone, allowing the attacker to get the sent the SMS code
- NIST (in SP 800-63) does not accept SMS codes as valid authentication because of how easy it is to hack

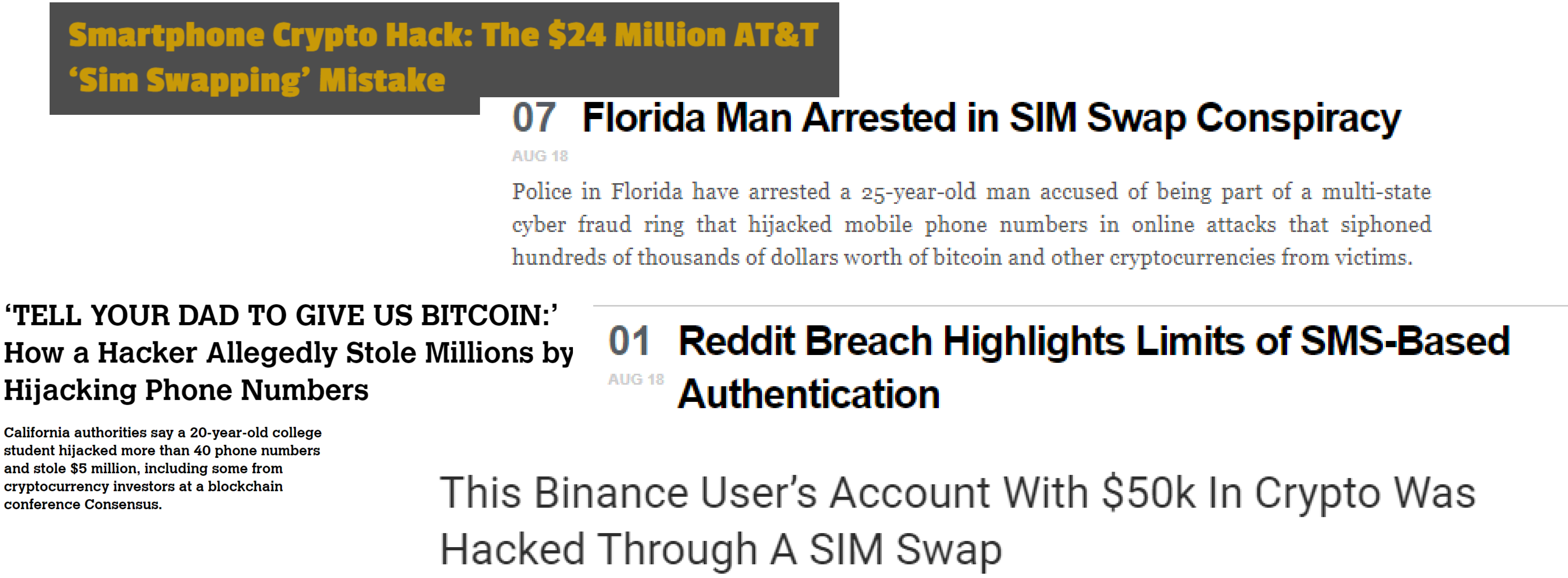


KnowBe4
Human error. Conquered.

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.

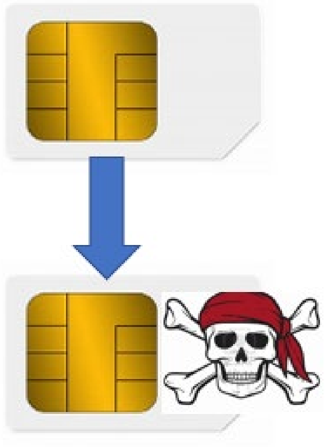
'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers

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 Attacks

SIM Swapping Attack

- Attackers (using different methods) successfully transfer your SIM information to their cell phone
- Often done by using social engineering:
  - To your cell phone network provider’s tech support
  - At local phone store or over phone
  - May start with successful vishing/phishing to victim to retrieve necessary cell phone account info
  - Information may be collected by reviewing victim’s social media accounts

MFA Hacks

SIM Swapping

SIM Swapping Attack (con't)

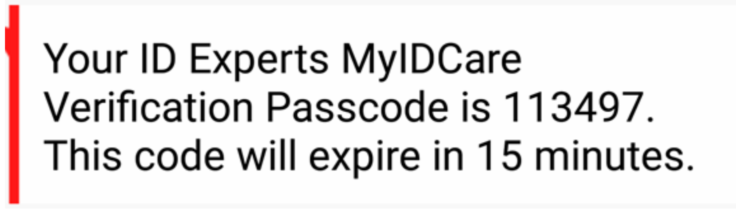
- Once SIM criminals have gathered enough info on victim, they call/visit the victim's cellphone provider and claim that the SIM card has been lost or damaged or buy new phones using your identity
- They activate another SIM card/number using your info
- Most vendors ask for additional information, that usually the thief has learned, such as account pin/password, address, last four of ssn, and/or answers to password reset questions
- Once transferred, thief has control of phone and SMS

MFA Hacks

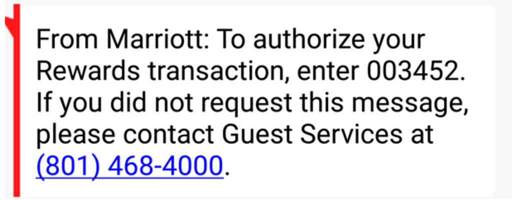
SIM Swapping

SIM Swapping Attack (con't)

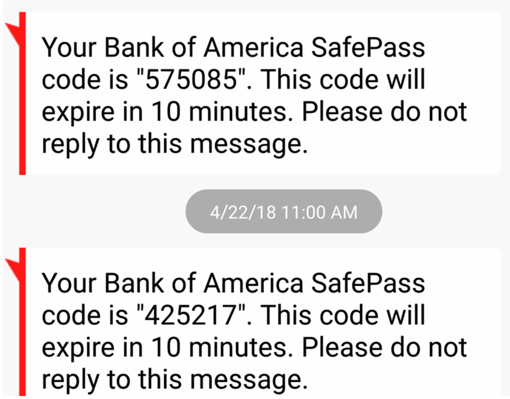
- Then thief logs into your MFA account, and gets sent SMS code, which they can respond with



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



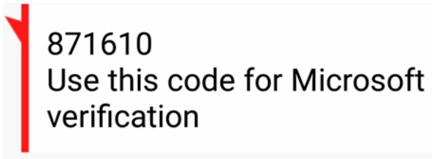
From Marriott: To authorize your Rewards transaction, enter 003452. If you did not request this message, please contact Guest Services at (801) 468-4000.



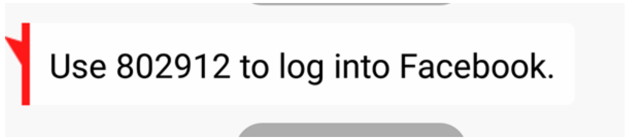
Your Bank of America SafePass code is "575085". This code will expire in 10 minutes. Please do not reply to this message.

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

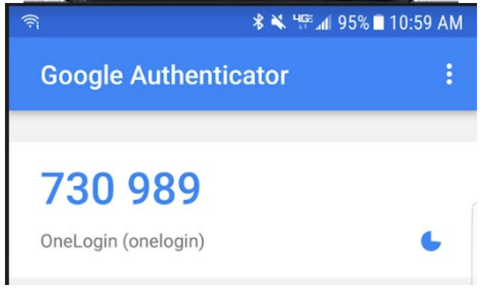
SIM Swapping

SIM 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

MFA Hacks

Duplicate Code Generator



Google Authenticator

730 989

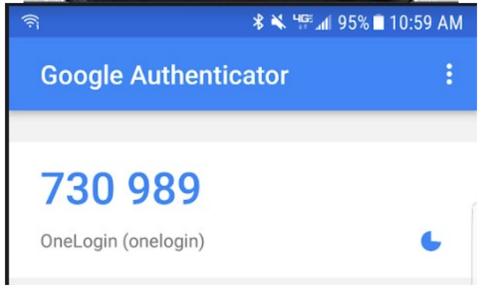
OneLogin (onelogin)

- 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



95% 10:59 AM

Google Authenticator

730 989

OneLogin (onelogin)

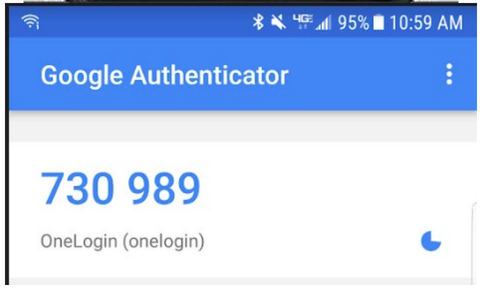
Real-Life Example: Chinese APT, RSA, and Lockheed Martin attack

KnowBe4
Human error. Conquered.

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

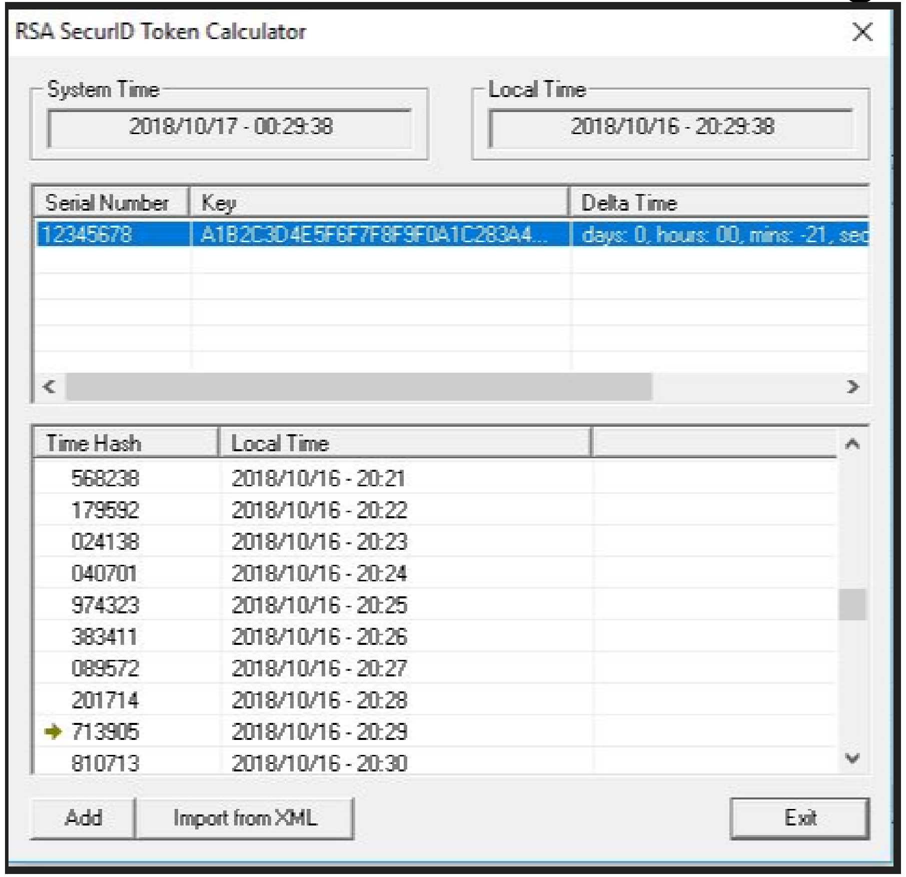

95% 10:59 AM

Google Authenticator

730 989

OneLogin (onelogin)

Taken from Cain & Abel hacking


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	A1B2C3D4E5F6F7F8F9F0A1C2B3A4...	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

KnowBe4
Human error. Conquered.

MFA Hacks

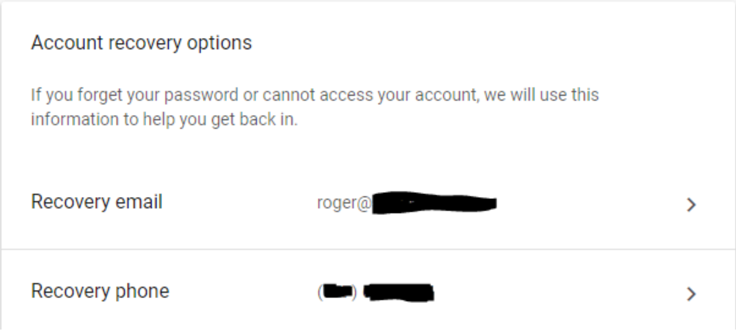
Not Required/ Downgrade Attacks

- 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

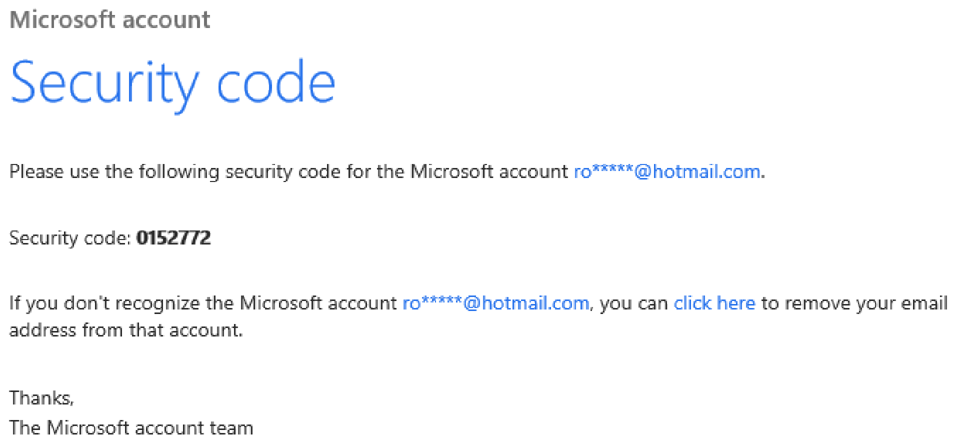


Account recovery options

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.

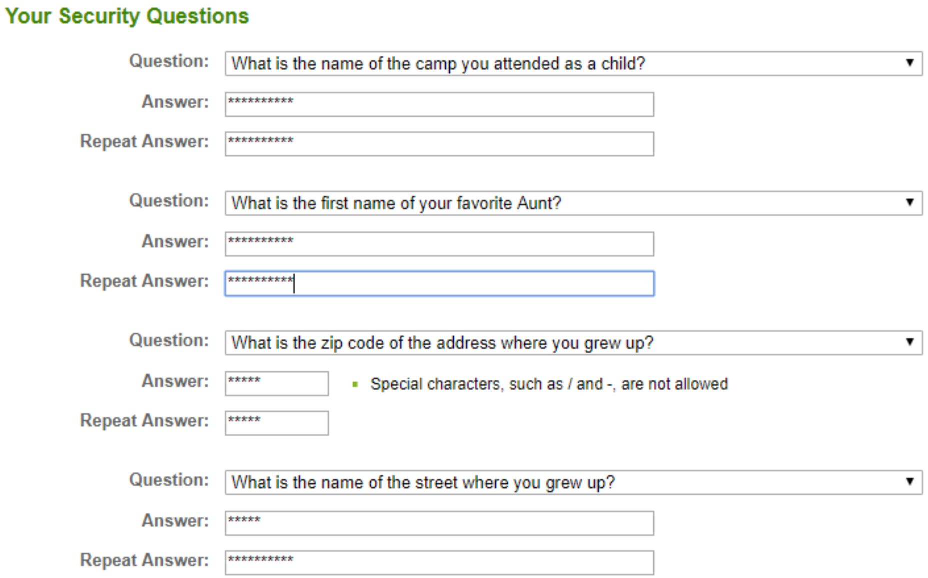
Thanks,
The Microsoft account team

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

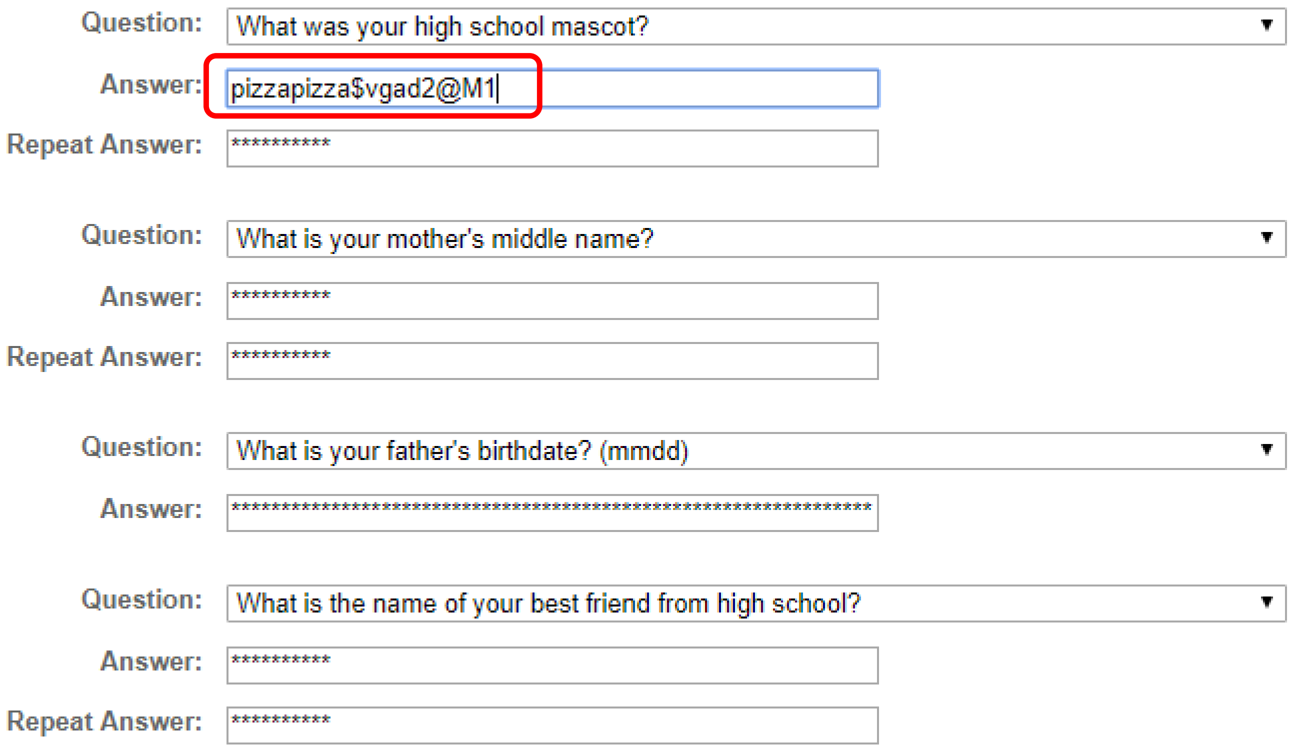
Problem: Answers can often be easily guessed by hackers

- 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)

Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack

- Hacker Must Know Your Email Address
- Hacker Must Know Your Phone Number

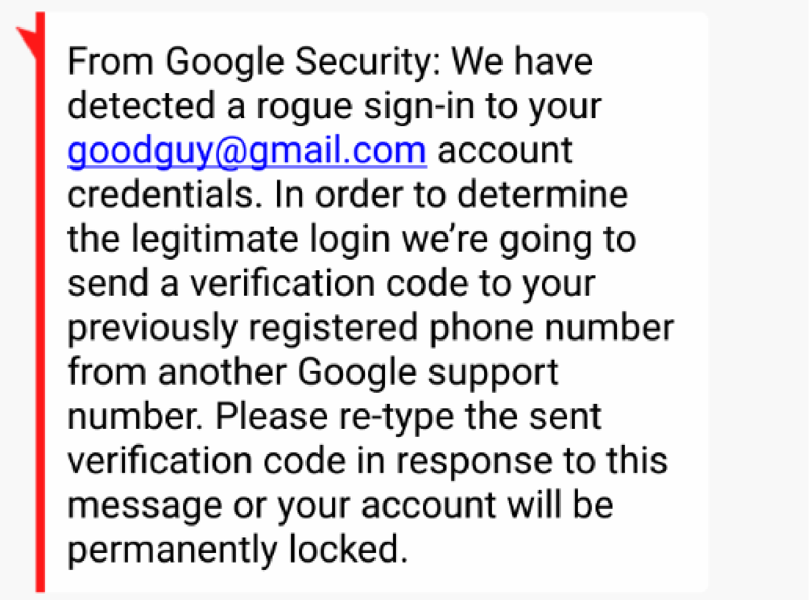
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack - 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.

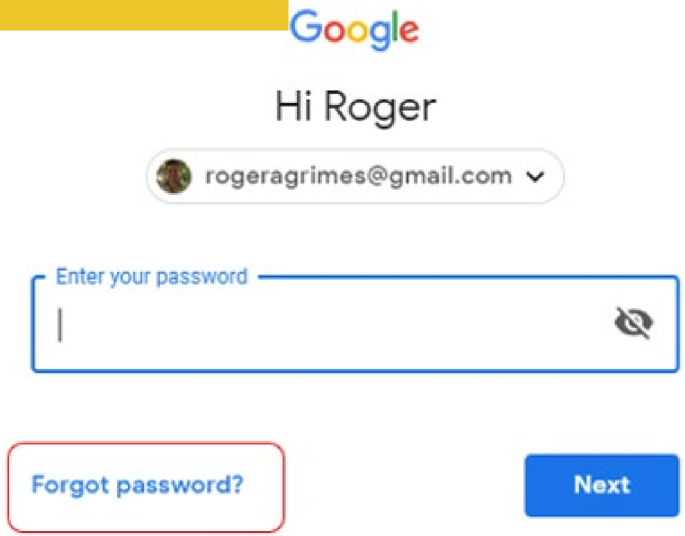
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack - Steps

2. Hacker forces your email account into SMS PIN recoverv



Google

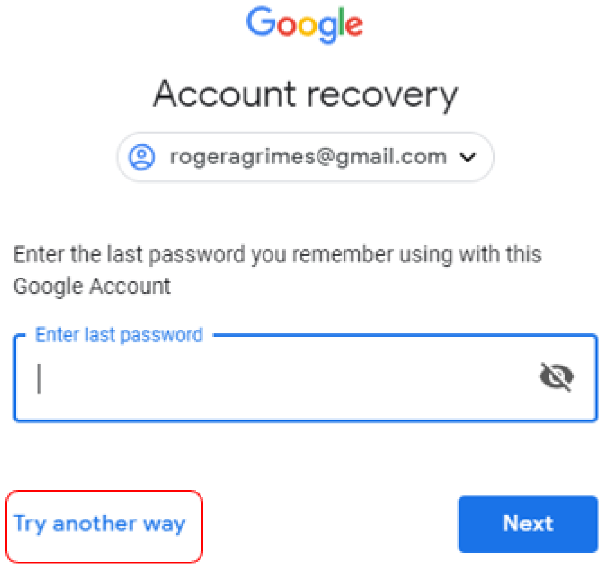
Hi Roger

rogeragrimes@gmail.com

Enter your password

Forgot password?

Next



Google

Account recovery

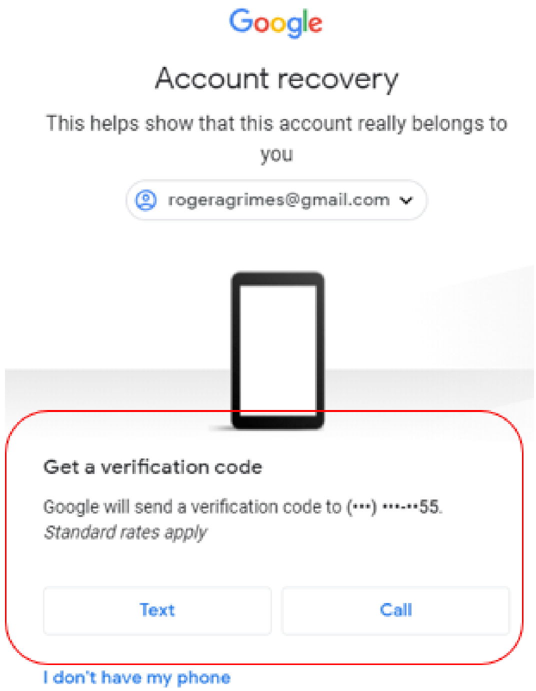
rogeragrimes@gmail.com

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

KnowBe4
Human error. Conquered.

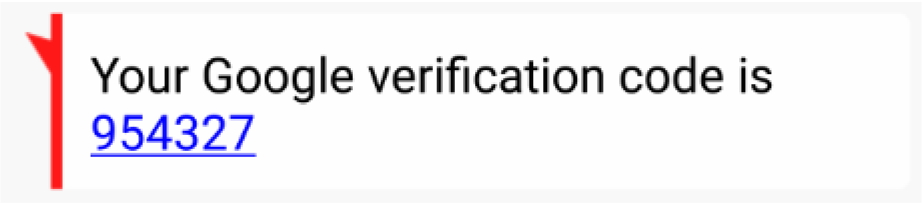
Rogue Recoveries

SMS Rogue Recovery

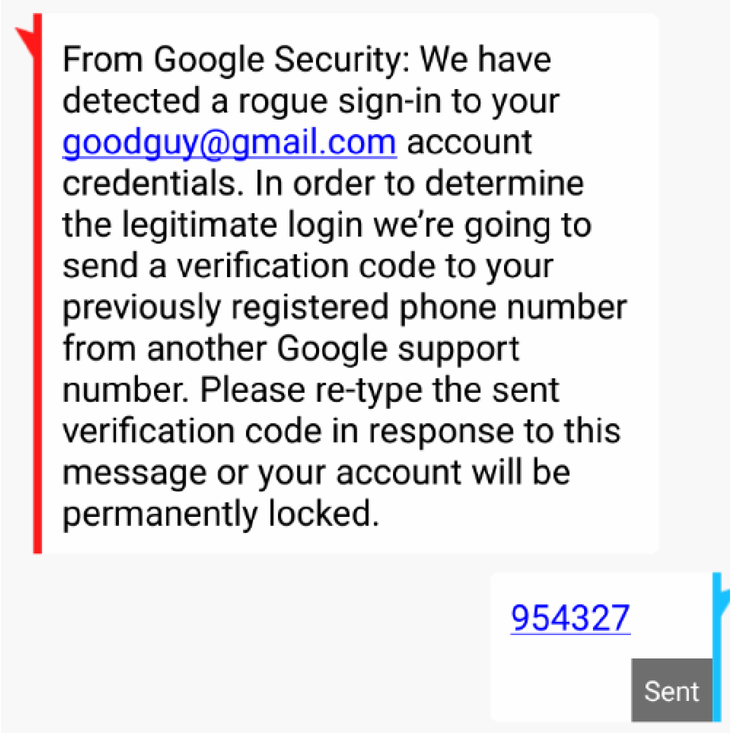
Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack - 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

SMS Recovery Hack - 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

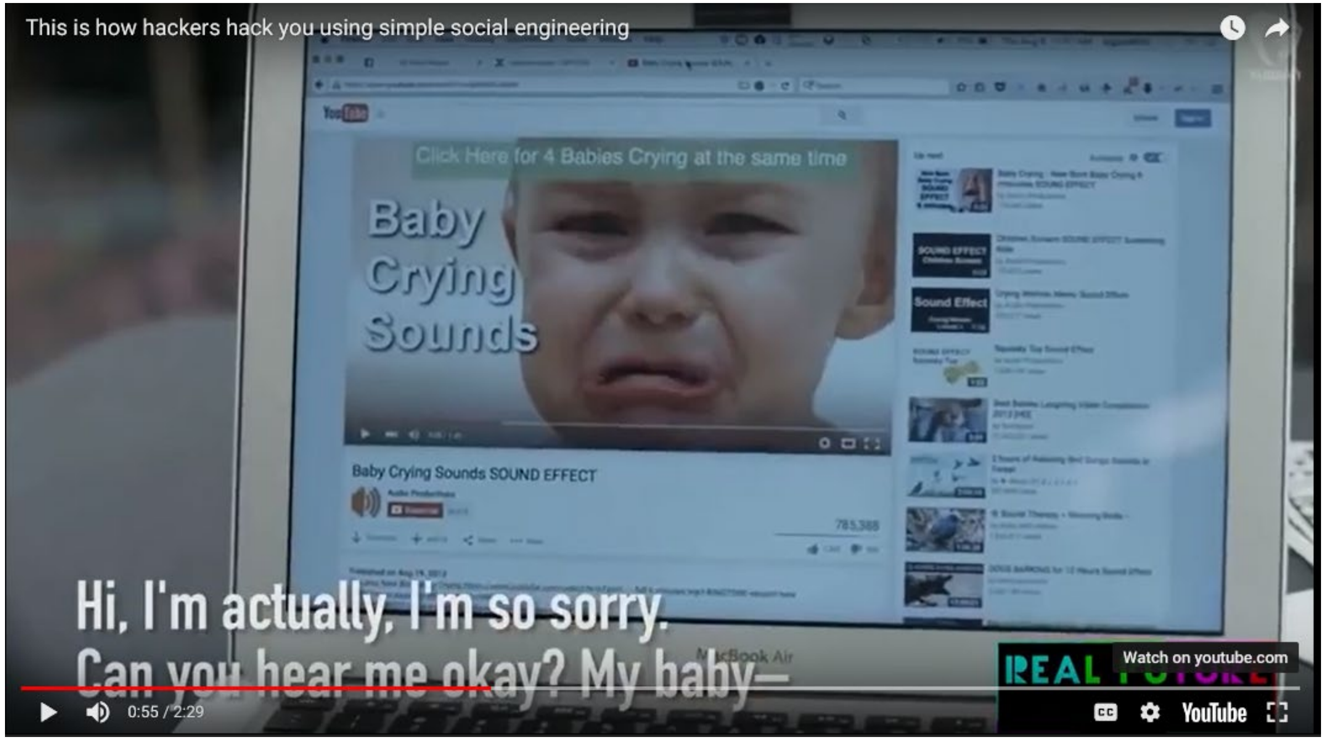
MFA Hacks

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

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

RSA®Conference2019

Defending Against MFA Attacks

Defending Against MFA Attacks

Defenses

Social Defenses

- 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

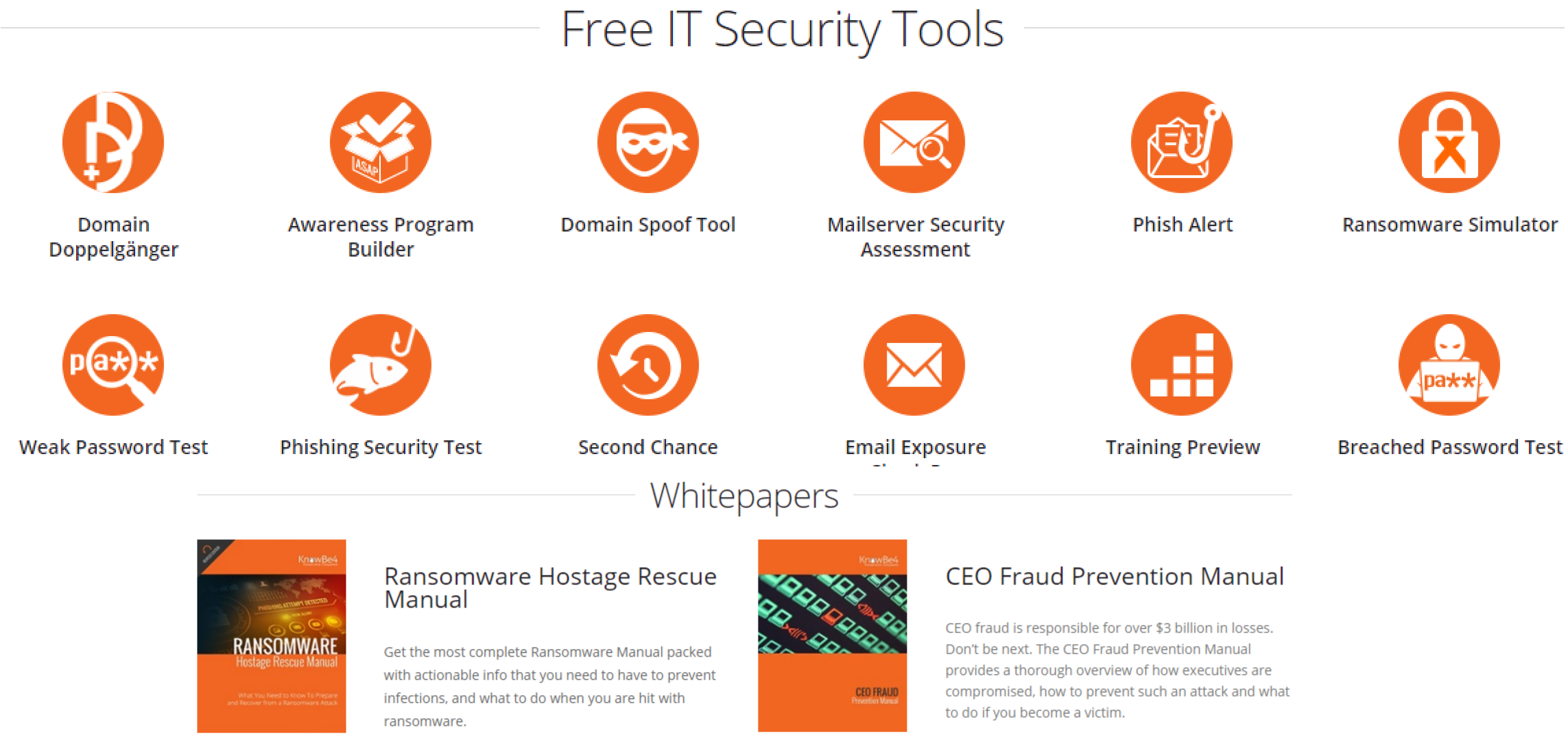
- MFA isn't unhackable
- MFA does not prevent phishing or social engineering from being successful
- MFA is good. Everyone should use it when they can, but it isn't unbreakable
- If you use or consider going to MFA, security awareness training has still got to be a big part of your overall security defense

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
- Training Preview
- Breached Password Test

Whitepapers

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.

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.

KnowBe4 Human error. Conquered. » Learn More at www.KnowBe4.com/Resources «

Apply What You Have Learned Today

- Today
  - Understand that any MFA solution can be hacked
  - Think about how you need to change technical and education solutions
- After
  - Update security awareness training to include “MFA hack” awareness
  - Make sure management understands MFA is not a security “Holy Grail”
  - Select best-fit, hack-resistant, MFA solutions