

KnowBe4
Human error. Conquered.

cadre
information security

Nuclear Ransomware & 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.

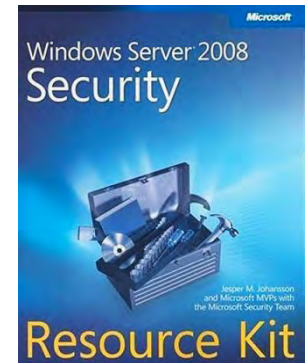
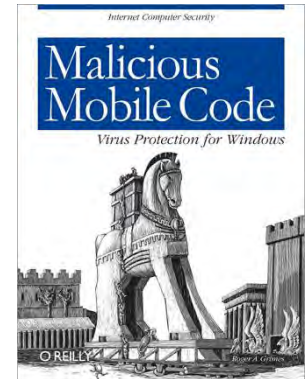
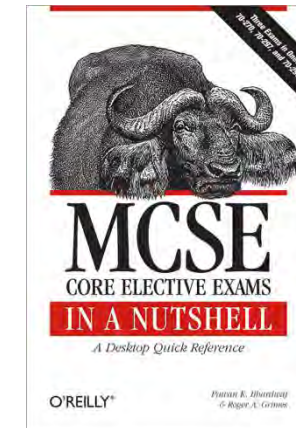
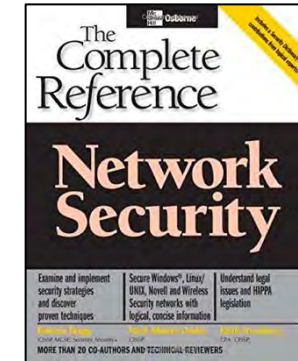
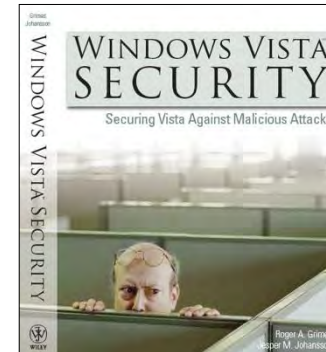
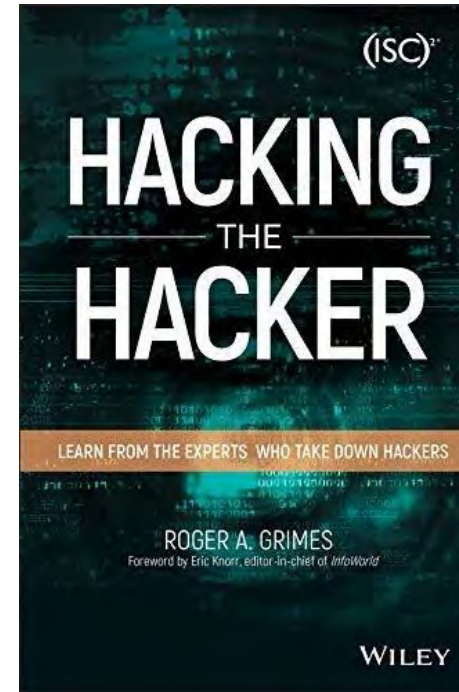
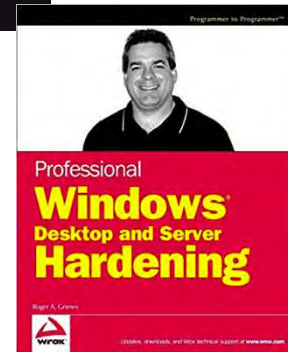
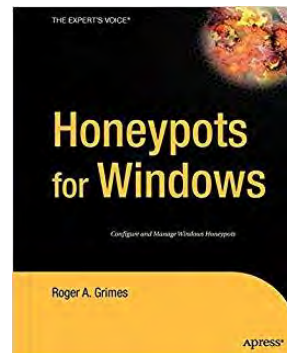
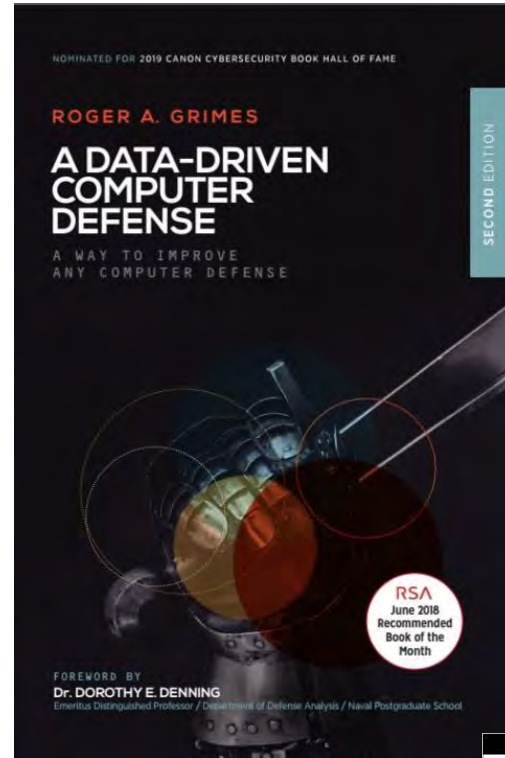
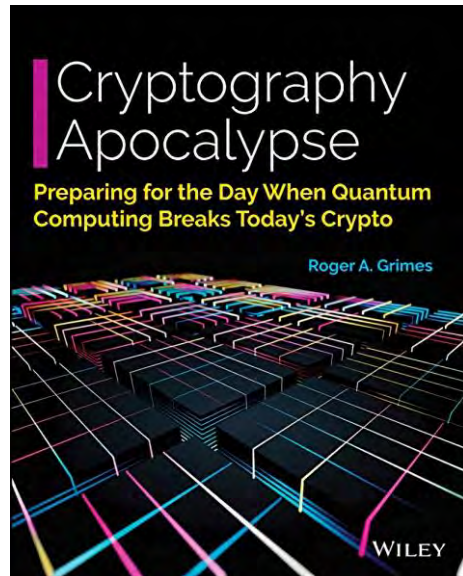
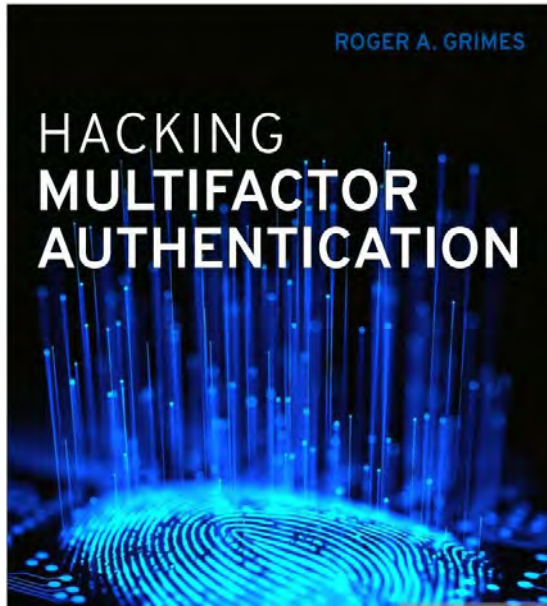
About Roger

- 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 12 books and over 1,100 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)

Certifications passed include:

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

Roger's Books



About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards



Agenda

- How Ransomware Is Becoming More Malicious
- Many Ways to Hack MFA

More Malicious Ransomware

Essentially:

- Ransomware crooks got tired of victims saying no
- They realized the access they had was the hacker “gold” and that they could do anything
- Encrypting data and holding it for hostage was the least of the victims worries now...

More Malicious Ransomware

Summary - Nuclear Badness

- Steal Intellectual Property/Data
- Steal Credentials
- Threatening Victim's Employees and Customers
- Using Stolen Data to Spear Phish Partners and Customers
- Public Shaming

Good luck having a good backup save you!

More Malicious Ransomware

Steal/Leak Data

- Ransomware now FREQUENTLY copies data before encrypting it
- Determines company's "crown jewels"
- Target database servers, stop processes, copies GB of data
- Threatens to post publicly, give to victim's competitors
- Ransomware groups involved so far: Zeppelin, Maze, Revil/Sodinokibi, Snatch, etc.

More Malicious Ransomware

Steal/Leak Data

CYBER NEWS BRIEFS

Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

→ encrypting it

→, Revil/Sodinokibi, Snatch,

22 Nov 2019



OODA Analyst

January 14, 2020

Maze ransomware operators that were allegedly stolen during the recent attack

Nemty ransomware makers may be latest to adopt data leak strategy

Sodinokibi Ransomware Publishes Stolen Data for the First Time

By [Lawrence Abrams](#)

January 11, 2020 06:07 PM 2

More Malicious Ransomware

Steal/Leak Data

- Ransomware now FREQUENTLY copies data before encrypting it

Boeing, Lockheed Martin, SpaceX Docs Leaked by Ransomware Gang

"The data was pilfered and dumped on the internet by the criminals behind the DoppelPaymer Windows ransomware, in retaliation for an unpaid extortion demand. The sensitive documents include details of Lockheed-Martin-designed military equipment—such as the specifications for an antenna in an anti-mortar defense system—according to a *Register* source who alerted us to the blueprints.

Other documents in the cache include billing and payment forms, supplier information, data analysis reports, and legal paperwork. There are also documents outlining SpaceX's manufacturing partner program."

More Malicious Ransomware

Threaten to Reveal Dirt – Real-World Example

Hackers double ransom demand to \$42M from Lady Gaga, Madonna's attorney, threaten Donald Trump

Attorney Allen Grubman – the most prominent entertainment attorney in the world, whose firm represents stars including [Lady Gaga](#), Madonna, [Mariah Carey](#), U2, [Bruce Springsteen](#), Priyanka Chopra and Bette Midler – was being shaken down by hackers who attacked his New York law firm for \$21 million until today.

Hacking group REvil got into his firm's server documents, including contracts and personal emails from a host of Hollywood and music stars. They also deleted or encrypted the firm's backups. The only way it can be decrypted is to pay the criminals for a key.

Ragnar Locker Ransomware Attacks Energy Company, Potentially Stealing 10TB in Data

More Malicious Ransomware

Auction Your Data– Real-World Example

Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format

1. Files pdf,docx,xlsx - 223288
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion

Minimum deposit:	\$5,000	Top bid:	—
Start price:	\$50,000	Blitz price:	\$100,000

Opened Time left: 6 days, 18 hours, 33 minutes and 12 seconds

More Malicious Ransomware

Steal/Leak Data

Example: **Travelex** ransomware attack – Dec. 2019

- Hackers broken in using missing server VPN patches (patches were available for months)
- Hackers in for 6 months before ransom kicked off
- 5GB of sensitive customer data including SSN, DOB, CC, etc.
- \$6M ransom
 - When Travelex first refused, ransom was \$3M, then hacker revealed he had customer data and wanted \$6M
- Travelex down at least 18 days
- Did not get fully operational until March 2020
- Put up for sale in April 2020 by parent company, partial due to ransomware event

More Malicious Ransomware

Steal Credentials

- Ransomware hackers search for every credential they can steal and re-use to maximize pressure, future pain, future financial gain
- Notpetya stole Windows/Active Directory credentials
 - But only to propagate
- Ransomware gangs now extract every found credential they can before revealing themselves and asking for ransom
- They don't usually tell you they have done it



06 The Hidden Cost of Ransomware: Wholesale Password Theft
JAN 20

More Malicious Ransomware

Steal Credentials

Example:

- Ransomware hackers were
- Used Trickbot trojan to collect

Indeed, Holden shared records of communications from VCPI's tormentors suggesting they'd unleashed Trickbot to steal passwords from infected VCPI endpoints that the company used to log in at *more than 300 Web sites and services*, including:

- Identity and password management platforms Autho and LastPass
- Multiple personal and business banking portals;
- Microsoft Office365 accounts
- Direct deposit and Medicaid billing portals
- Cloud-based health insurance management portals
- Numerous online payment processing services
- Cloud-based payroll management services
- Prescription management services
- Commercial phone, Internet and power services
- Medical supply services
- State and local government competitive bidding portals
- Online content distribution networks
- Shipping and postage accounts
- Amazon, Facebook, LinkedIn, Microsoft, Twitter accounts

More Malicious Ransomware

Threaten Victim's Employees

- Ransomware now targets employees of victim
- Notifies employees that they have the employee's logon credentials, SSN, personal info, etc.

More Malicious Ransomware

Threaten Victim's Customers

- Let's the victim's customers know that they have their logons and private data and will release publicly
- Sometimes actually extort the customer in addition to the company

More Malicious Ransomware

Threaten Victim's Customers

- Ransomware gang says PATIENTS of a compromised plastic surgery center must pay or else they will go public v **'Extremely uncomfortable'**

The hackers demanded a ransom payment from patients reported to the clinic that they also received hackers "threatening the public release of their" unspecified ransom demands are negotiated ;

Jere - who asked for his surname not be published - told BBC News someone calling themselves "the ransom guy" had told him:

- Vastaamo had refused to pay 40 bitcoin (£403,000)

About 300 records have already been published on the dark web, according to the Associated Press news agency.

Therapy patients cash after clinic da

On its website, the clinic calls the attack "a great crisis".

"I'm anxious about the fact that the attackers are in possession of my notes and conversations from those psychiatrist sessions," Jere said.

"Those notes contain things I'm not ready to share with the world.

More Malicious Ransomware

Use Stolen Data to Spear Phish Partners and Customers

- Ransomware gangs look through stolen data for information to use against your business partners and customers
- One of the fastest growing phishing segments

More Malicious Ransomware

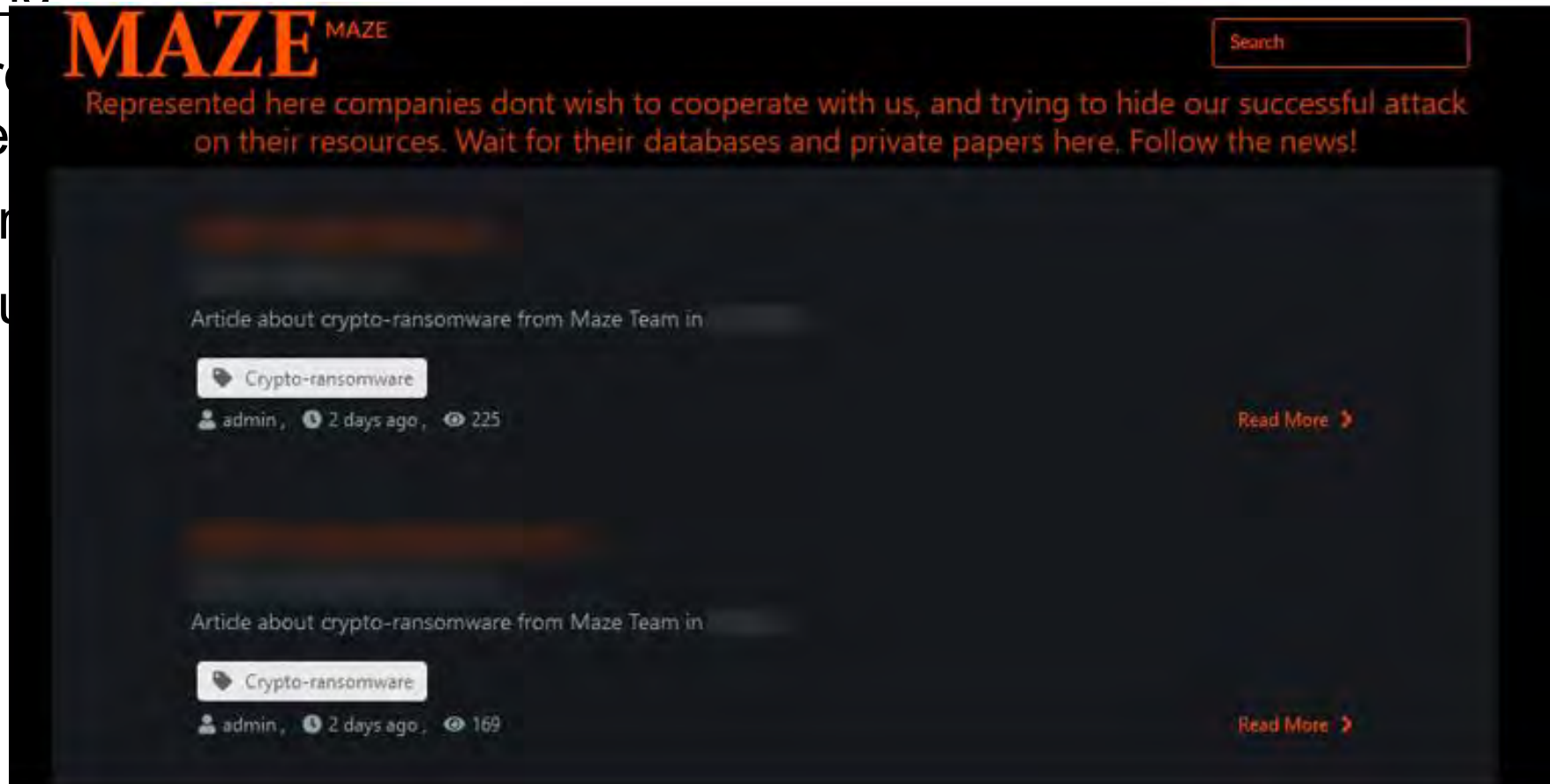
Public Shaming

- Ransomware will threaten to reveal publicly that you and your data has been compromised
- Maze ransomware group is one of the first to do this
- Created a public website/blog to display the names of companies they exploited
- List victim names
- Discuss data stolen
- Contact media sites to spread the news

More Malicious Ransomware

Public Shaming

- Ransomware compromise
- Maze ransomware
- Created a public shaming page



More Malicious Ransomware

Public Shaming

- Rarely reveal publicly that you and your data has been compromised
- Most of the first to do this
- Create a public shaming campaign to display the names of companies they exploited



A screenshot of a post on a data-leaking site. The post features a header for 'Kenneth Cole Productions' with the website 'kennethcole.com'. Below this, there is a message: 'Kenneth Cole Productions, good guys who value their reputation and their customers. Be like Kenneth Cole, take care of your nerves and money =)'. The post also includes a small table with columns for 'Email Address', 'Full Name', and 'Job Title', and a timestamp 'Feb 27, 2020'.

More Malicious Ransomware

Threaten Everyone – Real-World Example



Because of Robert Denison failed to take very simple security measures on his devices, I hacked into all employees google accounts that were hosted under the domain name of denisonyachtsales.com

All company leads, accounting archives, employee social security numbers, employee signatures including the data that sent from "clients" of Denison Yachting to the mailing accounts of the company is under my control.

So if you ever conducted business with Bob Denison, your private data might be in my hands right now.

What do I ask for?

I want Bob to send 15 BTC to this Bitcoin wallet address; 3J7sKP8dmoyisj2dcJoExfBUuvE5pPP9nT

What will happen if my demand won't be fulfilled? When the countdown here finishes, all the data that mentioned previously will be publicly available for anyone who visits this webpage.

Bob, this was your fault, don't make other people pay for your fault. For any questions, reach me at denisonextortion@protonmail.com

If this website shuts down, you can track the countdown on denisonextortion.com

0d 18h 11m 51s

More Malicious Ransomware

Future

- This is the new norm
- It may...somehow...actually get worse

Many Ways to Hack Multifactor Authentication

Introduction to multifactor 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

Network Session Hijacking

MFA Hacks

- 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

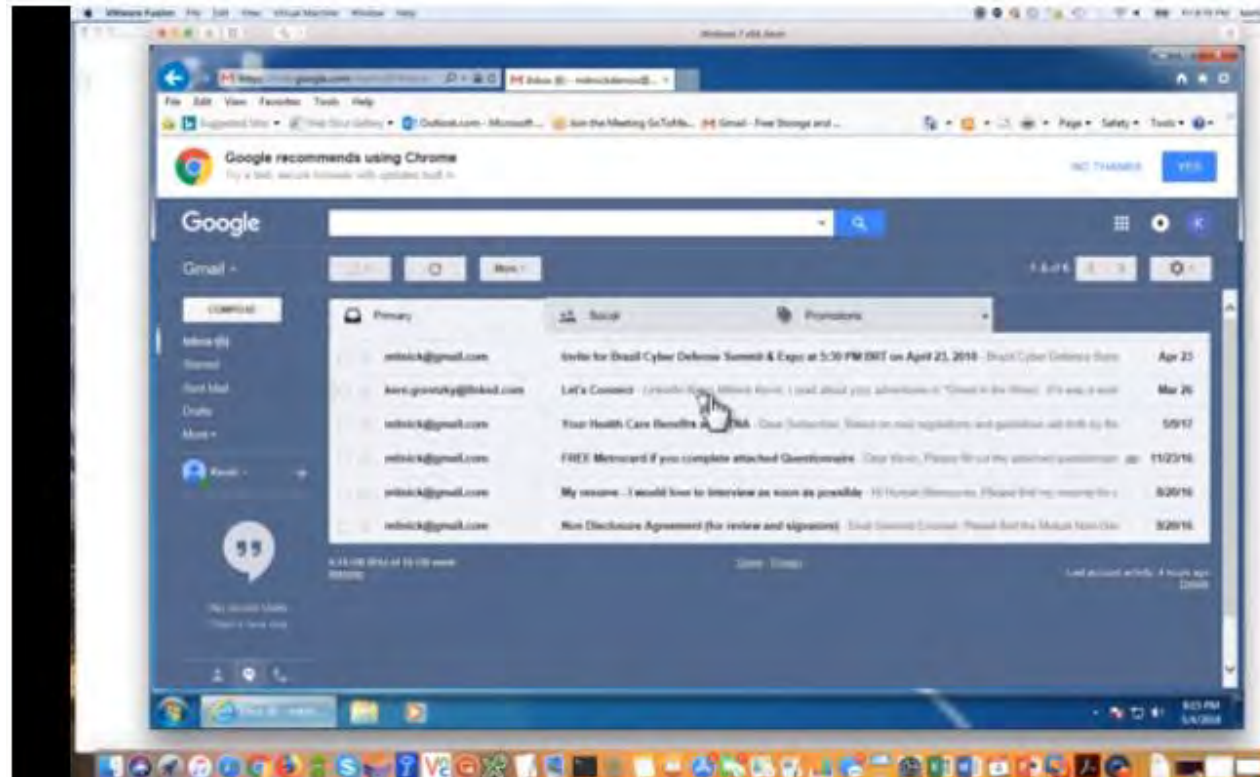
Network Session Hijacking Proxy Theft

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

MFA Hacks

Kevin Mitnick Hack Demo

Network Session Hijacking



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

MFA Hacks

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

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.

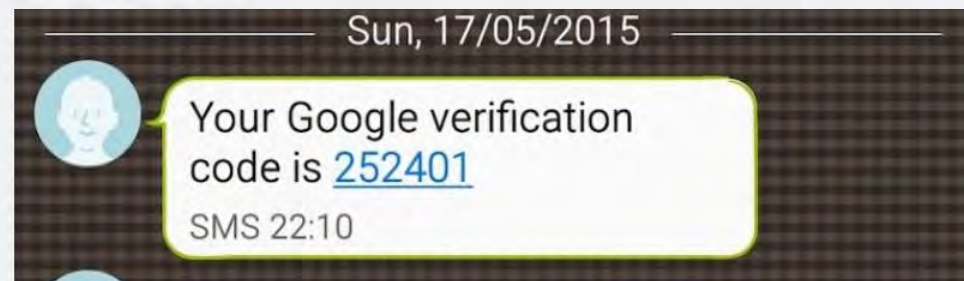
MFA Hacks

Network Session Hijacking

Real-World Example



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.



<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

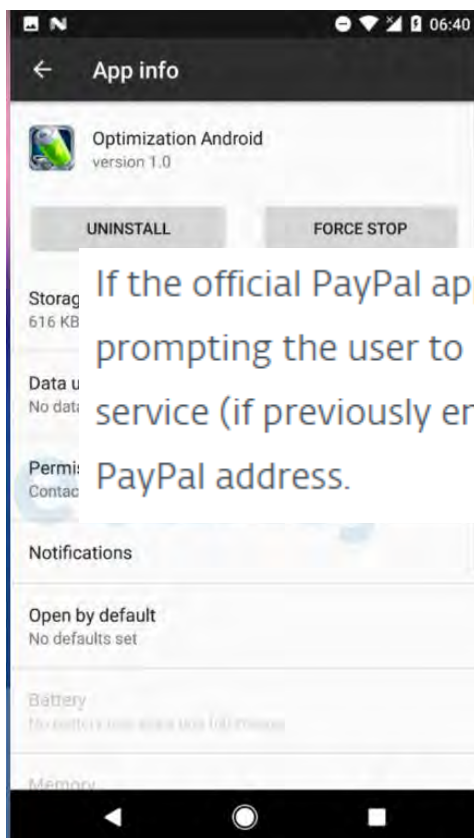
- Start up a second session that the user isn't even aware
 - Ex. Bancos trojans

The image shows a screenshot of a web browser displaying the Bank of America website. The browser's address bar shows the URL <https://www.bankofamerica.com>. The page features a news article titled "16 Feds Target \$100M 'GozNym' Cybercrime Network" dated MAY 10. The article text states: "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." A red box highlights the phrase "a stealthy banking trojan". To the right of the article is a login form with a "Sign In" button and links for "Forgot Online ID?", "Forgot Passcode?", "Security & Help", and "Enroll". Below the article are four promotional cards for financial services: "Find your closest financial center or ATM", "Schedule an Appointment", "I want cash back >" (4.5/5 (12,662) reviews), "I want travel rewards >" (4.4/5 (11,766) reviews), "I want a low intro APR offer >" (4.2/5 (12,255) reviews), and "I want premium rewards >" (4.4/5 (210) reviews). The bottom of the page shows images of Bank of America credit cards, including a BankAmericard and a Visa Premium Rewards card.

MFA Hacks

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>

Endpoint
Attacks

MFA Hacks

<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.

Endpoint Attacks

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)



MFA Hacks

SIM Swapping

SIM Basics

- SIM stands for **S**ubscriber **I**dentify **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

Food writer Jack Monroe 'loses £5,000 in phone-number hijack'

is accused of being part of a multi-state scheme of phone number hijacking that siphoned 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

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery

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

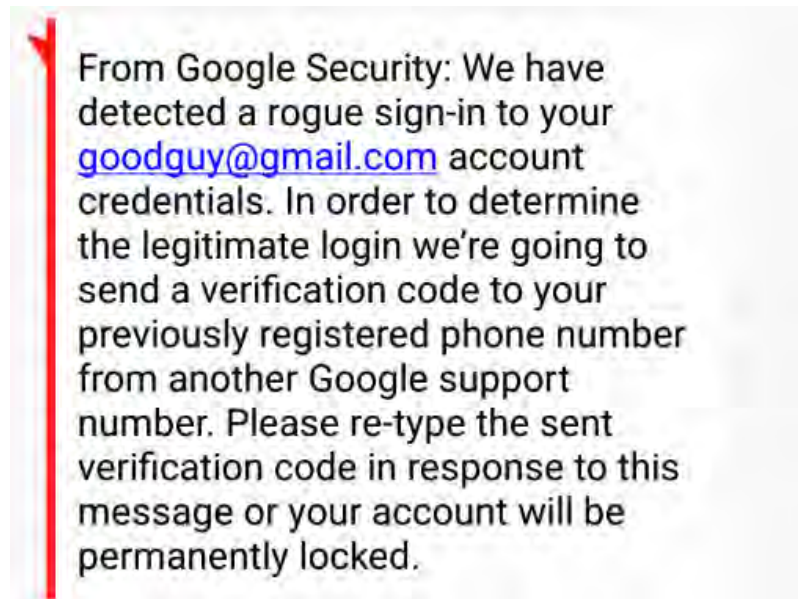
Rogue Recoveries

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



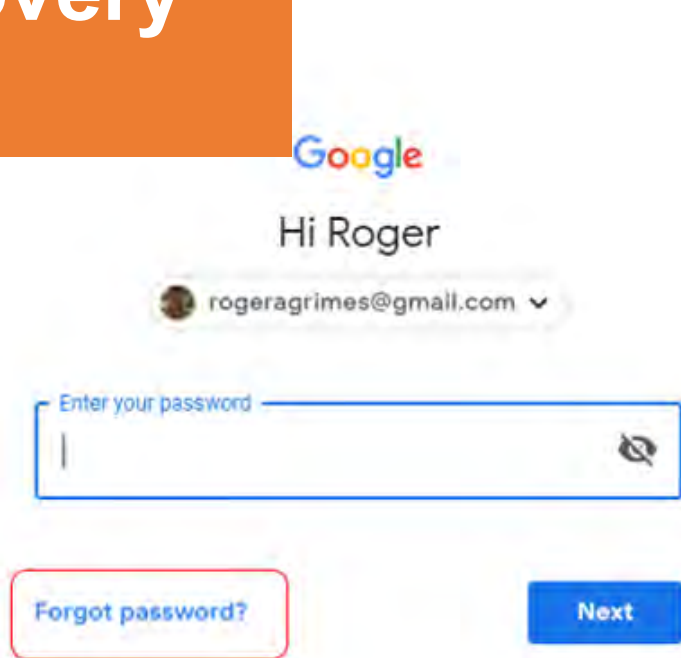
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

2. Hacker forces your email account into SMS PIN recovery



Google

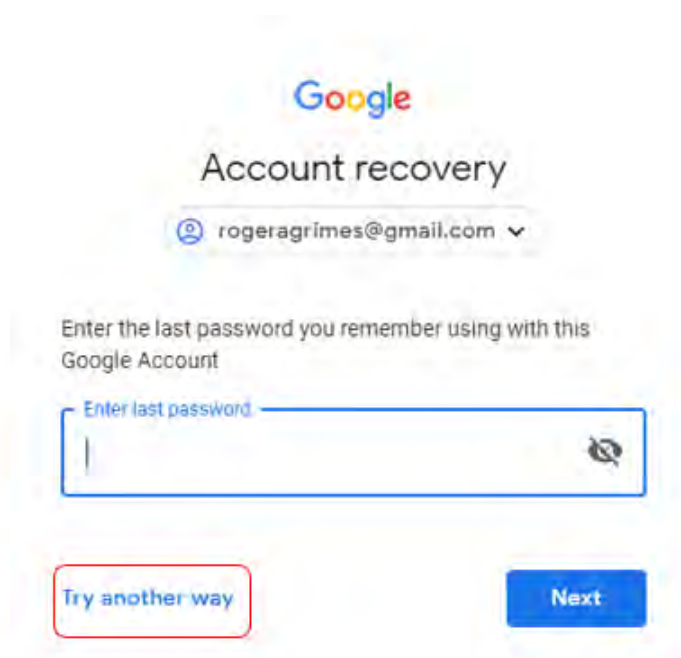
Hi Roger

rogeragrimes@gmail.com

Enter your password

Forgot password? Next

This screenshot shows the initial Google Account login screen. It features the Google logo, a personalized greeting 'Hi Roger', and the email address 'rogeragrimes@gmail.com'. There is a password input field with a placeholder 'Enter your password' and a 'Next' button. A 'Forgot password?' link is also visible.



Google

Account recovery

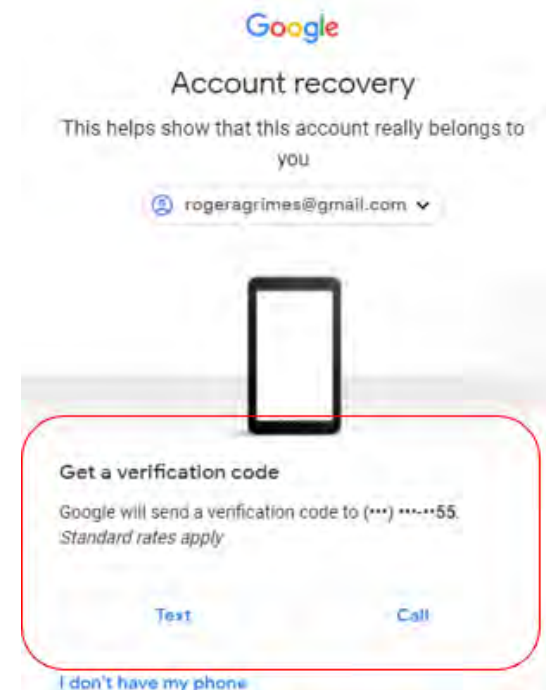
rogeragrimes@gmail.com

Enter the last password you remember using with this Google Account

Enter last password

Try another way Next

This screenshot shows the account recovery page where the user is prompted to enter their last password. It includes the Google logo, the text 'Account recovery', the email address 'rogeragrimes@gmail.com', and a password input field with a placeholder 'Enter last password'. There are 'Try another way' and 'Next' buttons.



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 (***). Standard rates apply.

Text Call

I don't have my phone

This screenshot shows the SMS verification step of the account recovery process. It features the Google logo, the text 'Account recovery', and a message: 'This helps show that this account really belongs to you'. The email address 'rogeragrimes@gmail.com' is displayed. A smartphone icon is shown above a red-bordered box containing the text 'Get a verification code' and 'Google will send a verification code to (***). Standard rates apply.'. Below this are 'Text' and 'Call' buttons, and a link 'I don't have my phone'.

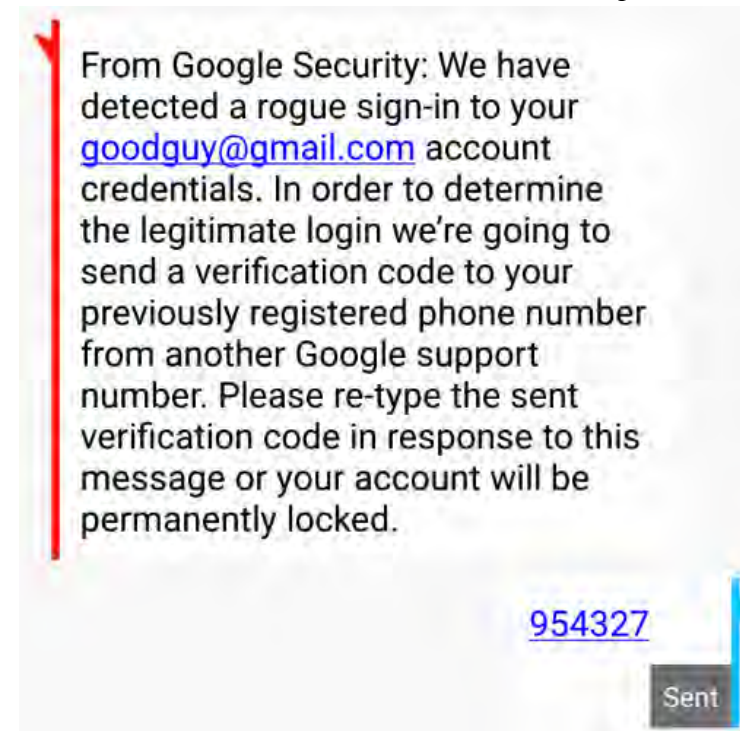
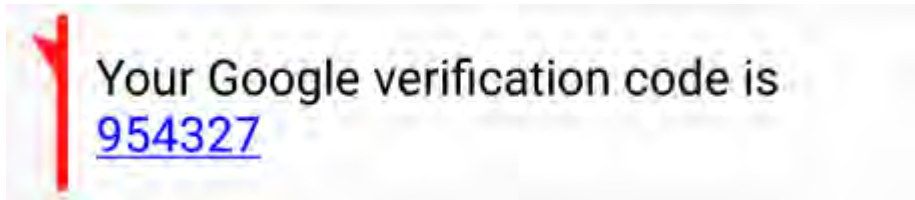
Rogue Recoveries

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



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

Hacking Into Your Email Using Recovery Methods

Then it got weird.

After confirming that he did not use his card in Miami, Gunst says the caller told him that the transaction had been blocked, and then asked him for his member number.

Gunst then received a legitimate verification pin from the bank's regular number via text, which he promptly read back to the caller -- not realizing that it was a password reset code.

The person on the line -- a scammer -- was in. She could access his account and began to read off recent transactions that Gunst had actually made, lending a bit more credibility to the call.

Then came the next question, which immediately set off a red flag: "We now want to block the pin on your account, so you get a fraud alert when it is used again. What is your pin?"

954327

ou then

<https://www.msn.com/en-us/news/crime/a-scam-targeting-americans-over-the-phone-has-resulted-in-millions-of-dollars-lost-to-hackers-dont-be-the-next-victim/ar-AAJpE2J>

Rogue Warnings

SMS Rogue Warnings

Fake Malicious Warnings

- Similar attack – Fake warning message
- Sends you to a fake, look-alike “verification” web page



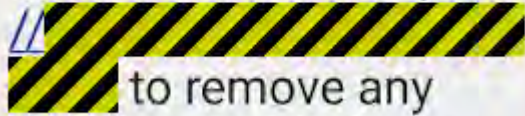
Hi Roger

Someone tried to log in to your Instagram account.

If this wasn't you, please use the following code to confirm your identity. Please [sign in](#):

453212

PayPal: Due to a recent failed payment request your account has been restricted. Visit: <https://>

 to remove any pending restrictions.

PAYPAL: We have detected unusual activity on your account, follow at <https://>

 to continue

MFA Hacks

- 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

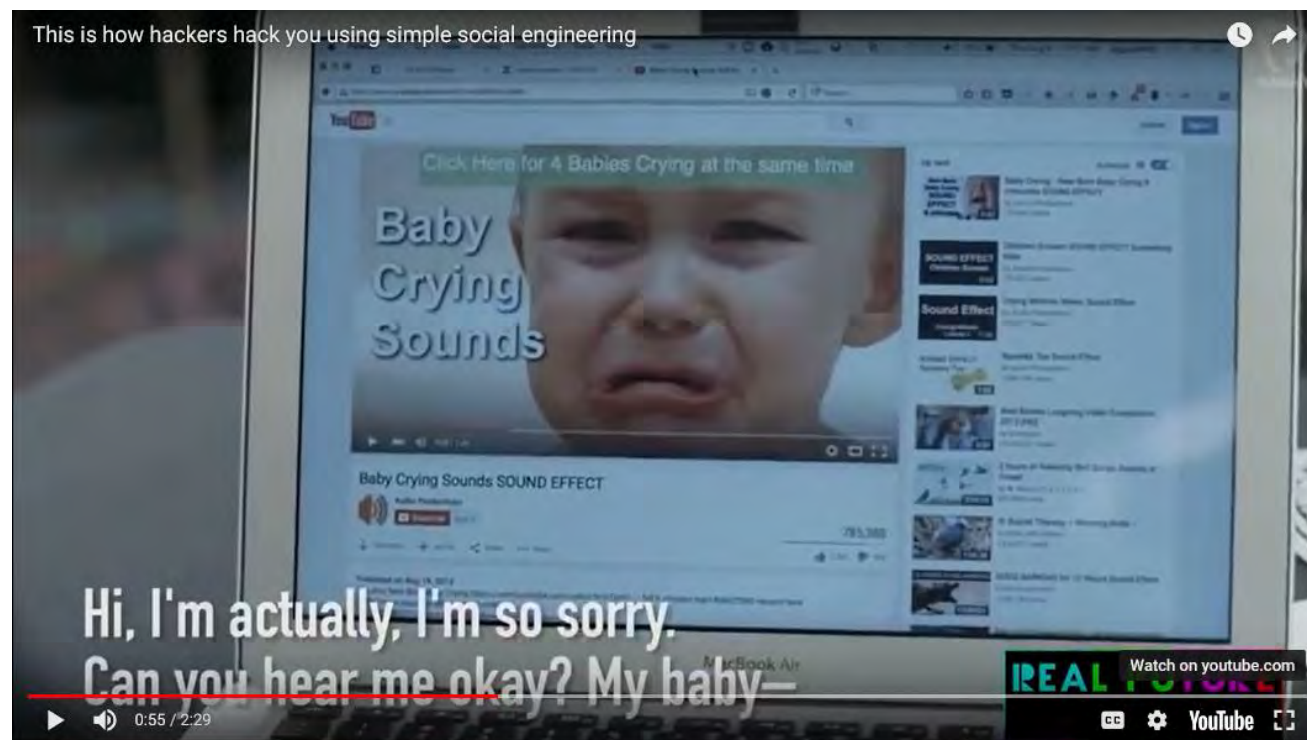
MFA Hacks

Social Engineer Tech Support

Great Example

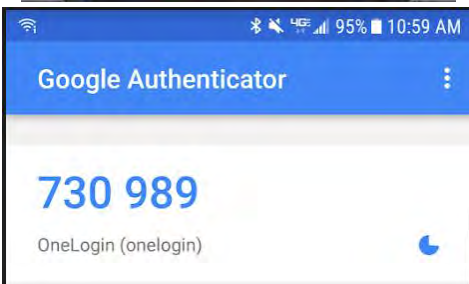
Check out the “Crying baby” social engineering live demo video:

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



MFA Hacks

Duplicate Code Generator



- 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)**

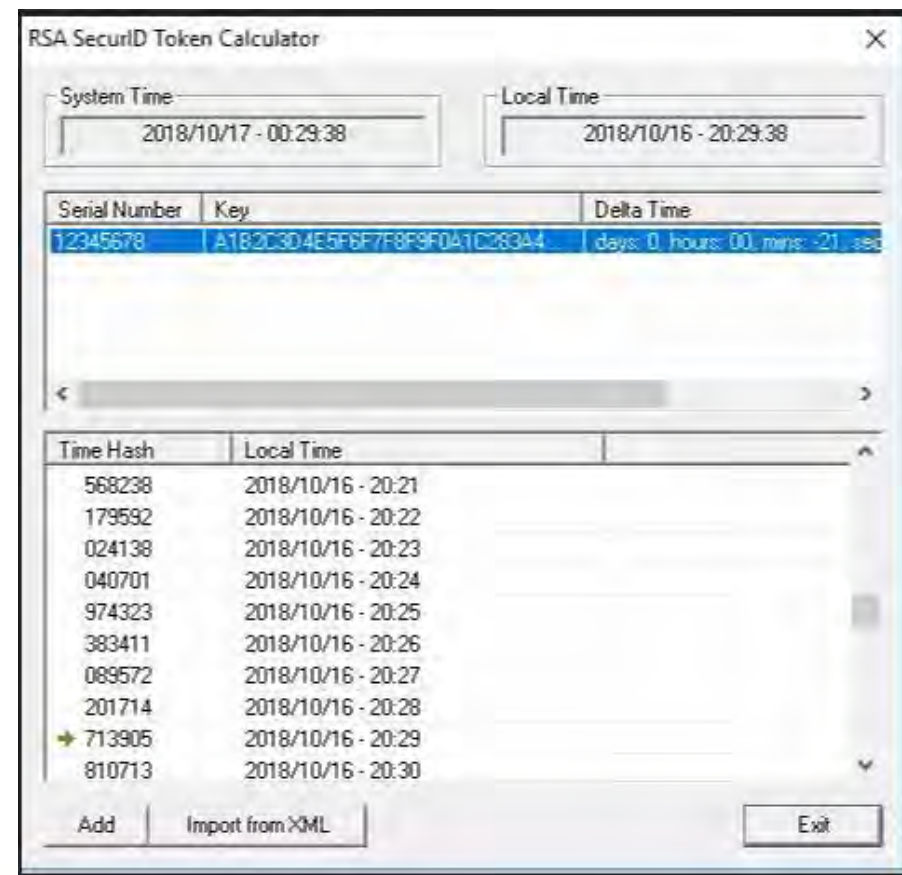
MFA Hacks

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

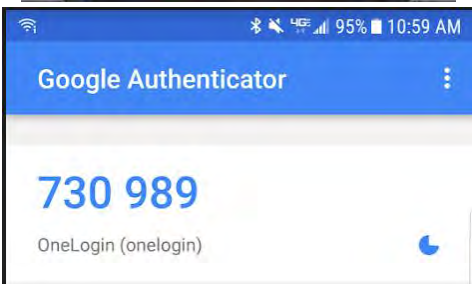
Taken from Cain & Abel hacking tool



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



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

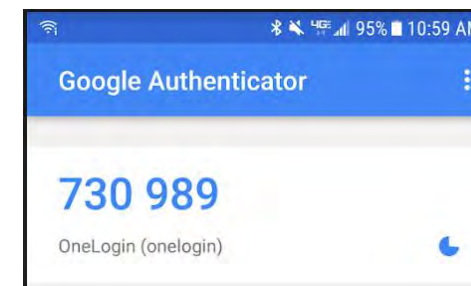
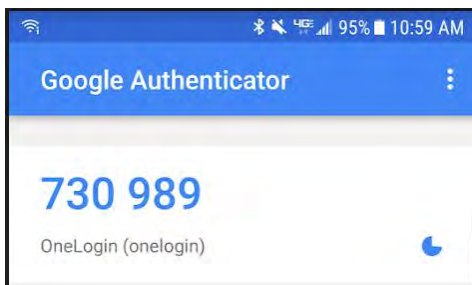
MFA Hacks

Duplicate Code Generator

- 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:



MFA Hacks

Duplicate Code Generator



Ir/coinbase

COMMENTS

Welcome to Reddit,
the front page of the internet.

BECOME A REDDITOR

and join one of thousands of communities.



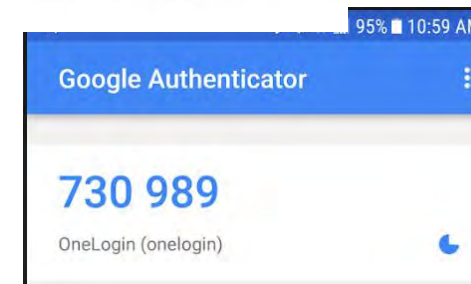
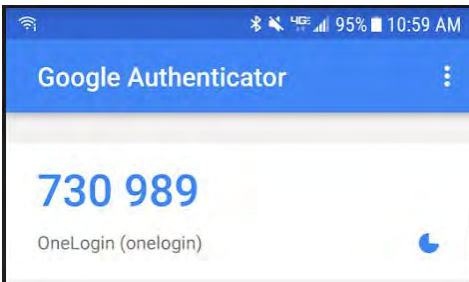
2-Factor can be hacked, apparently self.CoinBase

9

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.



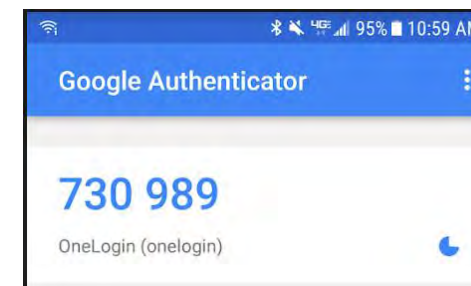
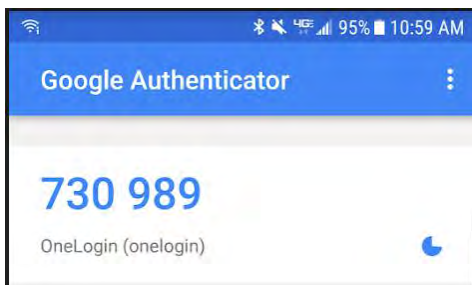
MFA Hacks

Duplicate Code Generator

- 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:



Duplicate Code Generator

The screenshot shows the Pharo Playground environment. The code in the playground is as follows:

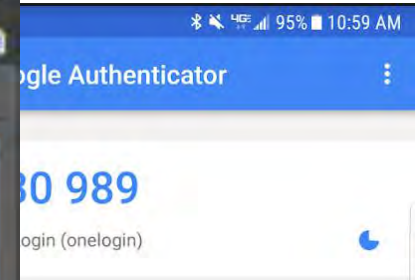
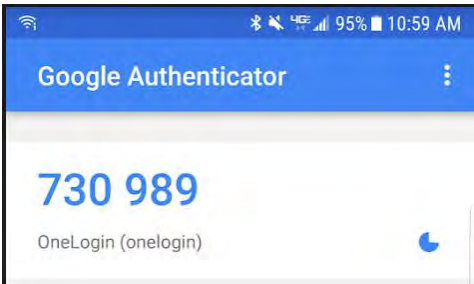
```
authenticator := GoogleAuthenticator new.  
authenticator base32Secret: 'HXDMVJECJJWSRB3HWIZR4IFUGFTMXBQZ'.  
authenticator nextPadded. "1672812"
```

Below the code, the Inspector on a GoogleAuthenticator instance is open, showing the following variables and values:

Variable	Value
self	a GoogleAuthenticator
codeLength	6
hashMode	SHA1
period	30

enticator

the barcode below:



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@██████████ >

Recovery phone (██████████) ██████████ >

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:

Answer:

Repeat Answer:

Question:

Answer:

Repeat Answer:

Question:

Answer: Special characters, such as / and -, are not allowed

Repeat Answer:

Question:

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:

Answer:

Repeat Answer:

Question:

Answer:

Repeat Answer:

Question:

Answer:

Question:

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



MFA Hacks

- 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 ...

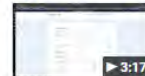
<https://blog.elcomsoft.com/.../breaking-apple-icloud-reset-password-and-bypass-two-f-...> ▼
Nov 28, 2017 - Who am I to tell you to use **two-factor authentication** on all accounts that support it? This recommendation coming from someone whose ...

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 ...



Buggy MFA

MFA Hacks



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

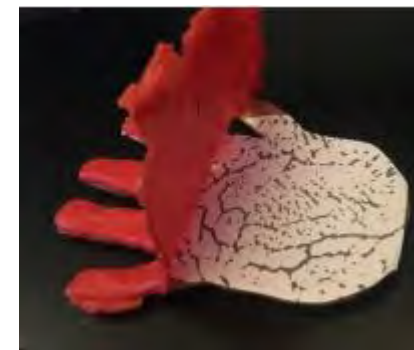
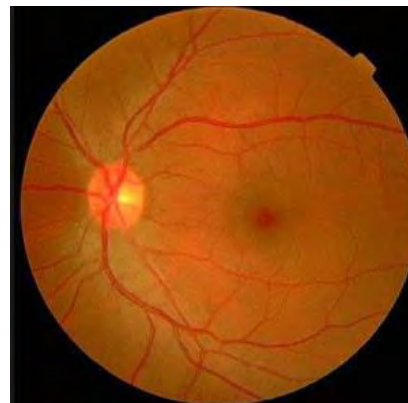
Buggy MFA

MFA Hacks

Physical Attacks

Biometric

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



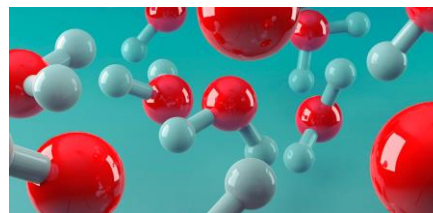
By [Catalin Cimpanu](#) for [Zero Day](#) | January 5, 2019 -- 13:49 GMT (05:49 PST) | Topic: [Security](#)

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



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!



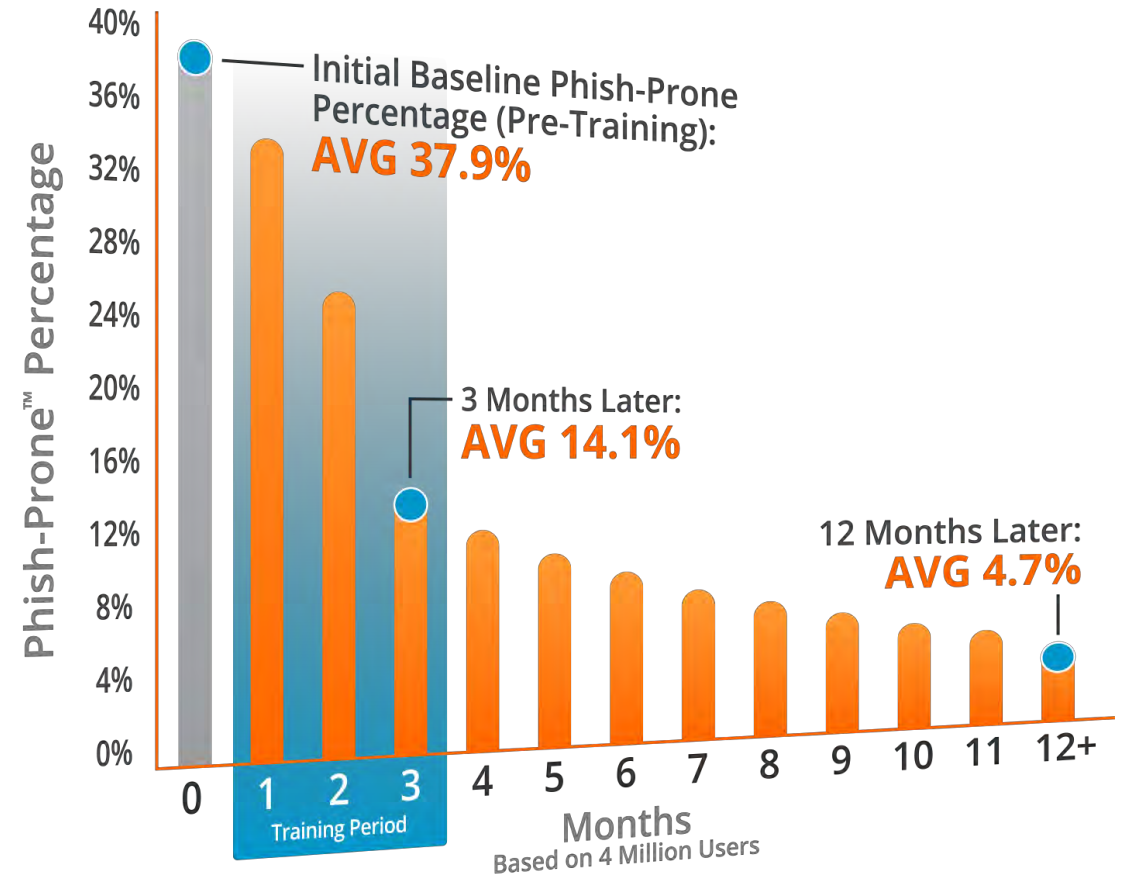
Generating Industry-Leading Results and ROI

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

87% Average Improvement

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

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 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.



Source: 2020 KnowBe4 Phishing by Industry Benchmarking Report

Questions?

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

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)

<https://www.linkedin.com/in/rogeragrimes/>