KnowBe4
Human error. Conquered.

Hacking Multifactor Authentication

An IT Pro’s Lessons Learned After Testing 150 MFA Products

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes

Data-Driven Defense Evangelist

KnowBe4, Inc.

Twitter: @RogerAGrimes

LinkedIn: https://www.linkedin.com/in/rogeragrimes/

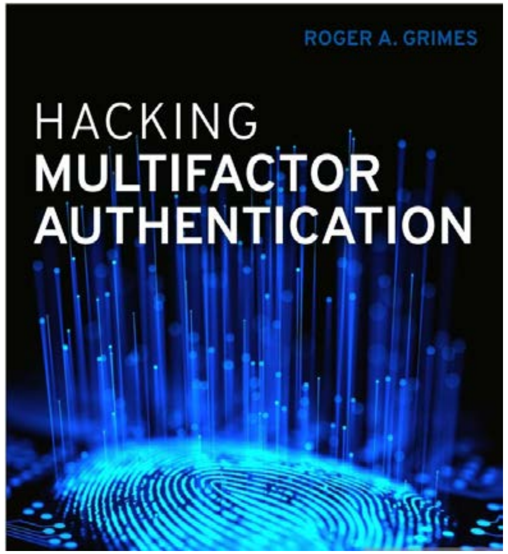
About Roger

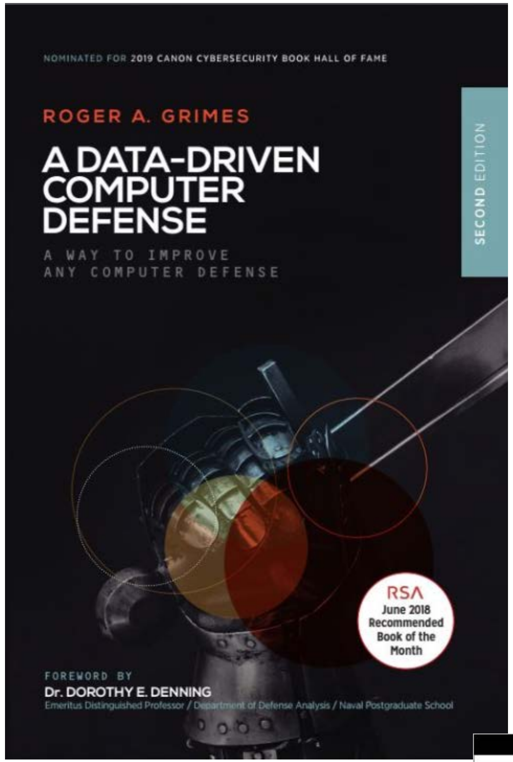
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,100 magazine articles
- *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)

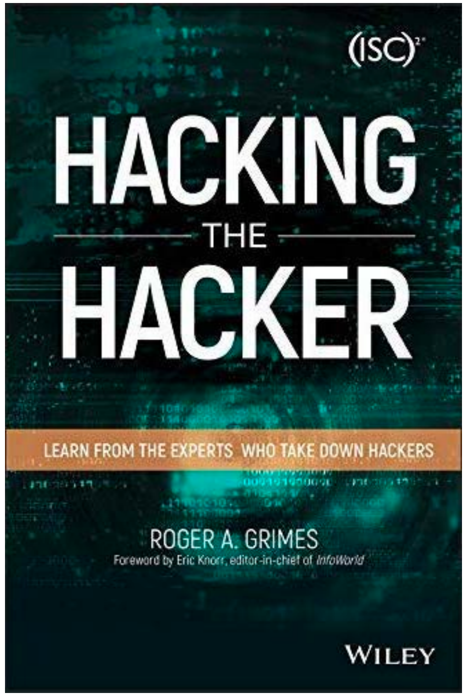
Certification exams passed include:

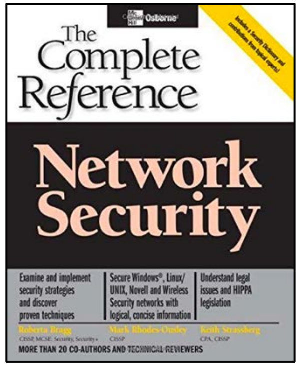
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

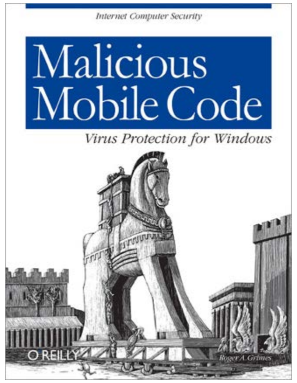
Roger’s Books

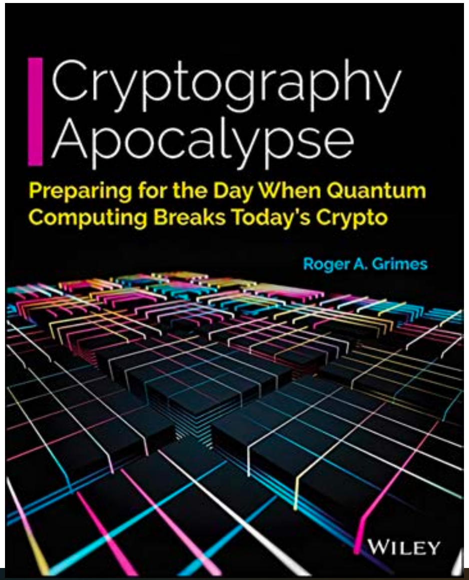


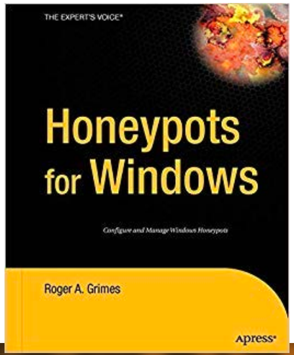

NOMINATED FOR 2019 CANON CYBERSECURITY BOOK HALL OF FAME
ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
SECOND EDITION
RSA June 2018 Recommended Book of the Month
FOREWORD BY
Dr. DOROTHY E. DENNING
Emeritus Distinguished Professor / Department of Defense Analysis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

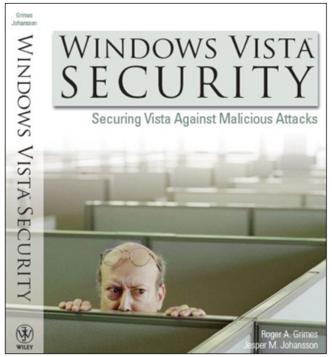

(ISC)²
HACKING THE HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

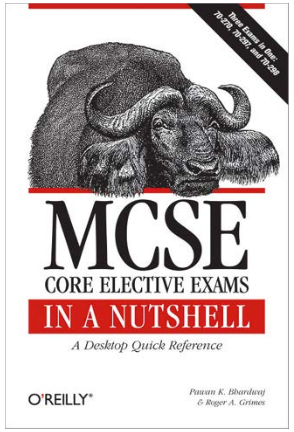


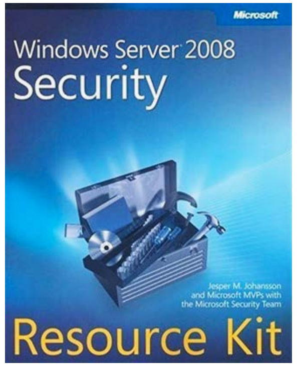


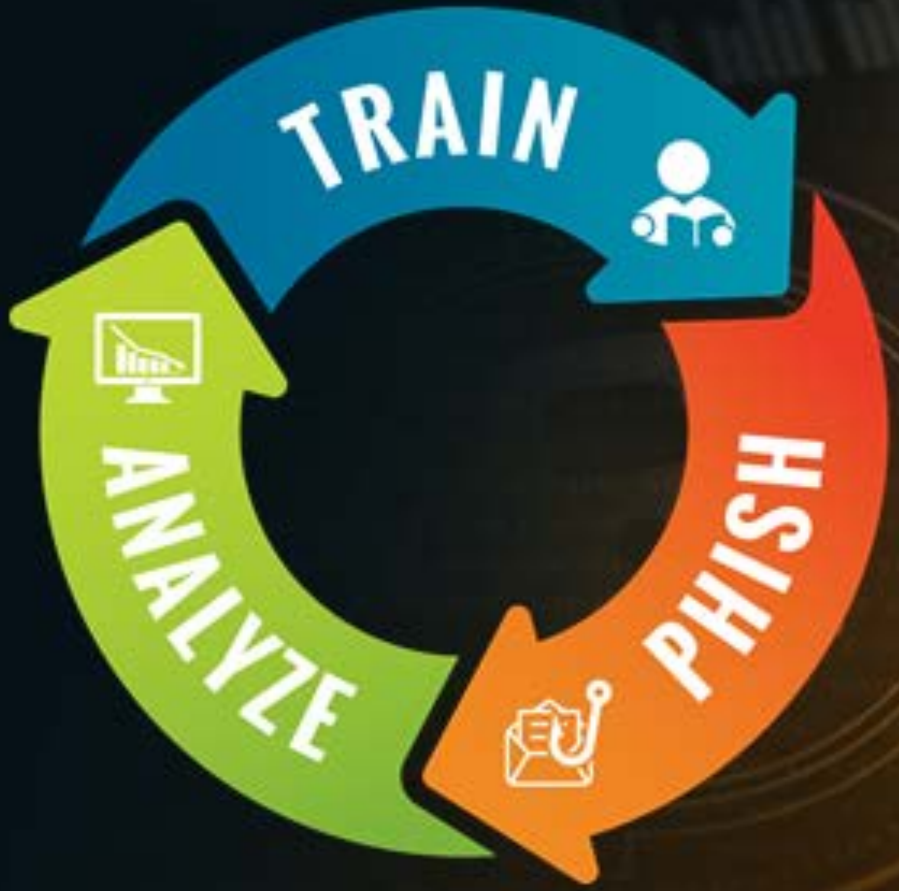

Cryptography Apocalypse
Preparing for the Day When Quantum Computing Breaks Today's Crypto
Roger A. Grimes
WILEY






MCSE
CORE ELECTIVE EXAMS
IN A NUTSHELL
A Desktop Quick Reference
O'REILLY
Pawan K. Bhardwaj & Roger A. Grimes


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



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

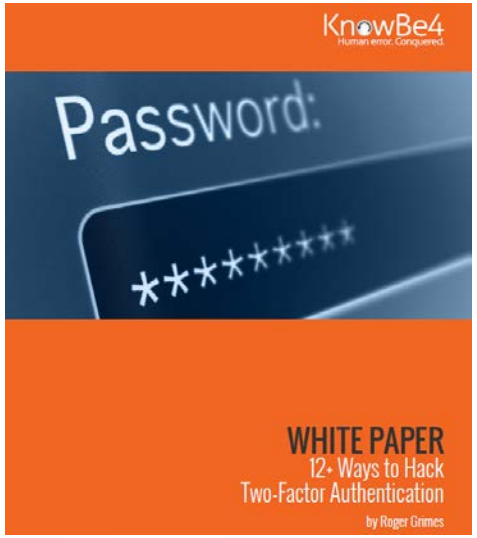
Agenda

- General Types of MFA
- How to Hack MFA
- The Good, the Bad, and the Ugly
- How to Pick the Right MFA Solution

Background

Bio

- Penetration tester for over 20 years
- Worked on dozens of MFA and MFA hacking projects
- Wrote **Hacking Multifactor Authentication** book (Wiley)
  - https://www.amazon.com/Hacking-Multifactor-Authentication-Roger-Grimes/dp/1119650798
- Delivered **Many Ways to Hack MFA webinar** for years
  - https://info.knowbe4.com/webinar-12-ways-to-defeat-mfa
- Wrote free **12 Ways to Hack 2FA ebook**
  - https://info.knowbe4.com/12-way-to-hack-two-factor-authentication
- Helped develop the **Multifactor Authentication Security Assessment** tool
  - https://www.knowbe4.com/multi-factor-authentication-security-assessment



Background

Hacking MFA

- As part of the webinar and book I had many MFA vendors ask me if I could hack their product
  - I could
- I threat modeled every product discussed in my book
  - 135 at my book’s publishing date
  - And dozens of others since
- I can hack any MFA solution at least a few ways
- Most many ways, many over 10 ways

Background

Hacking MFA

Most common question about MFA I get asked is:

“Can X MFA solution be hacked?

Answer: Yes!

Second most common question is:

What is THE best MFA solution?

Answer: There is no “best” single solution for everyone, but there is a best methodology for choosing the best MFA solution for you

That’s what this webinar is all about

Agenda

- General Types of MFA
- How to Hack MFA
- The Good, the Bad, and the Ugly
- How to Pick the Right MFA Solution

Types of MFA

Authentication Factors

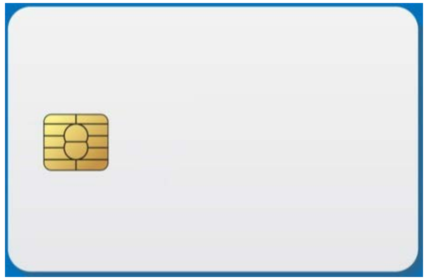
- Something You Know
  - Password, PIN, Connect the Dots, etc.
- Something You Have
  - USB token, smartcard, RFID transmitter, dongle, etc.
- Something You Are
  - Biometrics, fingerprints, retina scan, smell
- Contextual, behavioral analytics, actions, location, etc.

Types of MFA

- Single Factor (1FA)
  - Not all MFA is really “MFA”
- Two Factor (2FA)
- Multifactor (MFA), 2 or more factors

- Hardware-focused
- Software-focused

Types of MFA



Hardware-Based MFA Examples

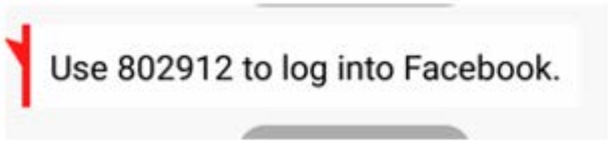
- USB devices
- Stand-alone credit card-style devices
- Smartcards
- Wireless (contactless) vs physical connection
- Smart watches

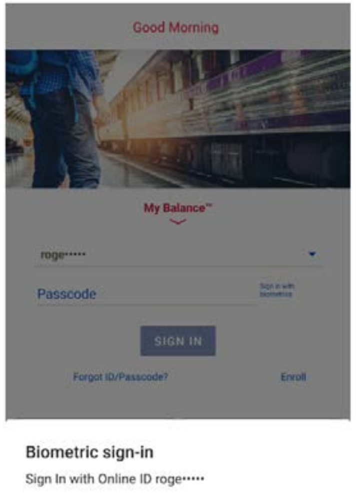
- Cell Phone
  - Known as "phone as a token"

Types of MFA

Phone-Based MFA

- Gaining in popularity
- SMS-based
    - Not super secure
- Phone-app
    - Push-Notification
    - Pretty secure but not fool-proof
- Voice-based


Use 802912 to log into Facebook.


Good Morning

My Balance™

roge••••••

Passcode

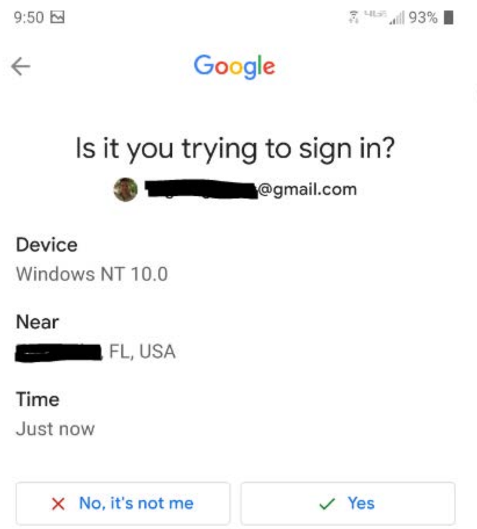
Sign in with biometrics

SIGN IN

Forgot ID/Passcode? Enroll

Biometric sign-in

Sign In with Online ID roge••••••


9:50 93%

Google

Is it you trying to sign in?

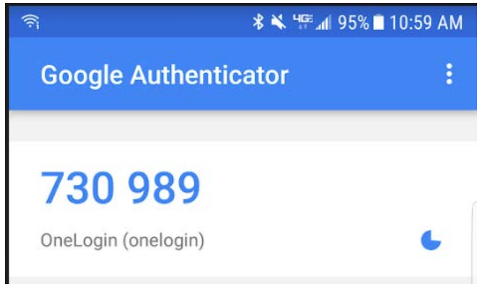
[redacted]@gmail.com

Device
Windows NT 10.0

Near
[redacted] FL, USA

Time
Just now

✕ No, it's not me ✓ Yes


95% 10:59 AM

Google Authenticator

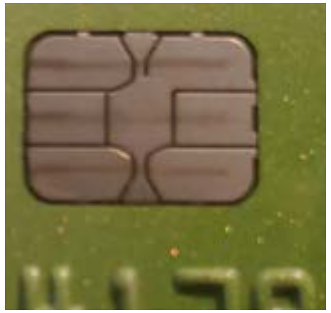
730 989

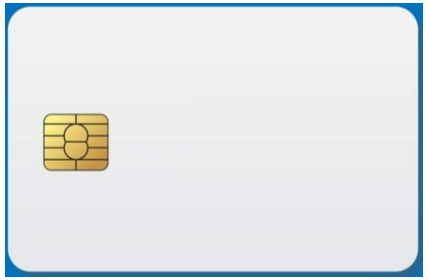
OneLogin (onelogin)

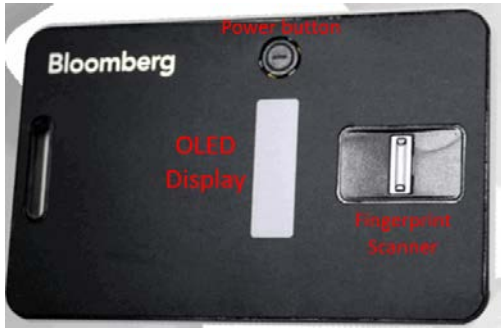
Types of MFA

<ins>Token-Based MFA</ins>

- Wired or wireless
- Smartcards
- USB-style tokens
- Credit-card style
- RFID cards
- FIDO keys
- Yubikeys







Types of MFA

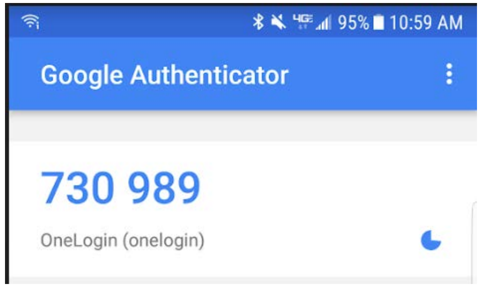
One-Time Password (OTP) MFA

- Uses random “seed value”, algorithm/hash and event or time to generate one-time password (OTP) code
  - Ex: Every 10 minutes, new code, but not tied to current time
  - Ex: Push a button, new code every use, etc.

Types of MFA

Time-based One-Time Password MFA

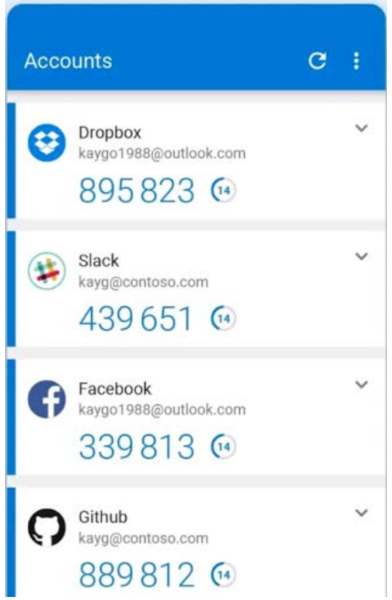
- Uses random “seed value”, algorithm, and current time to generate one-time password (OTP) code


95% 10:59 AM

Google Authenticator

730 989

OneLogin (onelogin)


Accounts

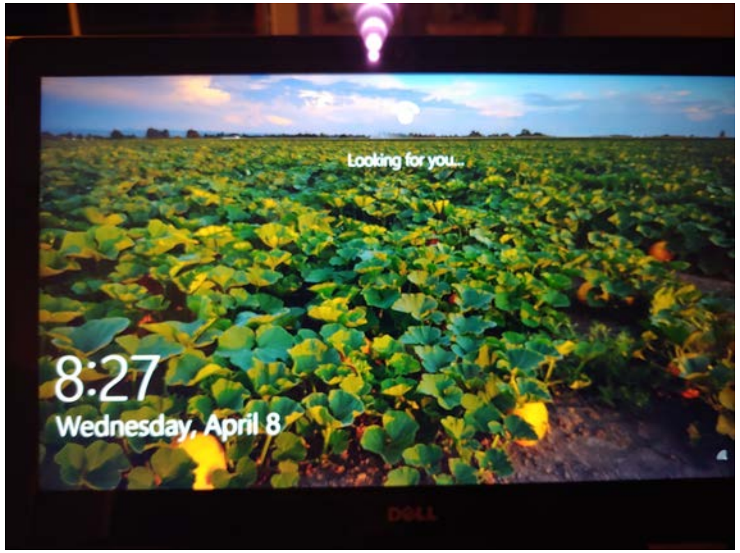
Dropbox
kaygo1988@outlook.com
895 823

Slack
kayg@contoso.com
439 651

Facebook
kaygo1988@outlook.com
339 813

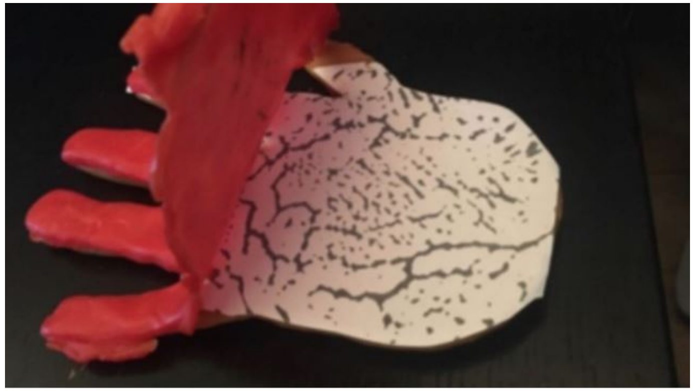
Github
kayg@contoso.com
889 812

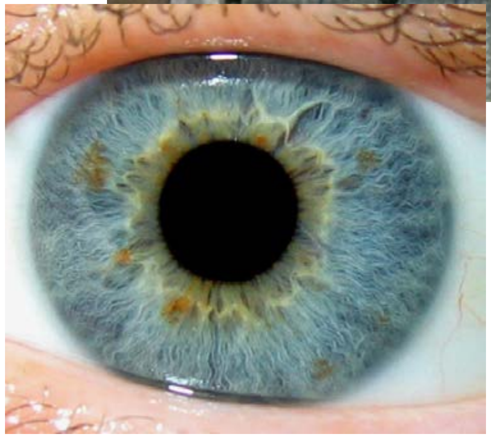
Types of MFA



Biometric Examples

- Physical
  - Eye, hand, face
- Behavioral
  - Keystroke dynamics
- Contactless

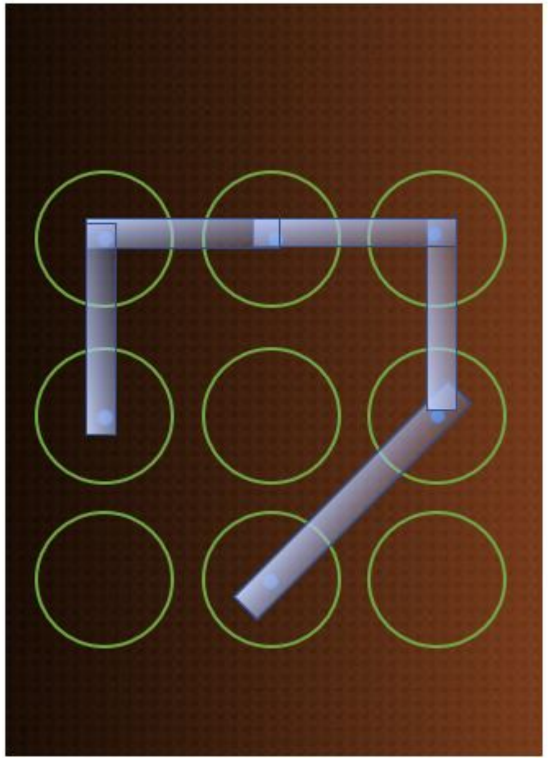




Types of MFA

Something You Know Examples

- Passwords, PINs
- Connect the Dots

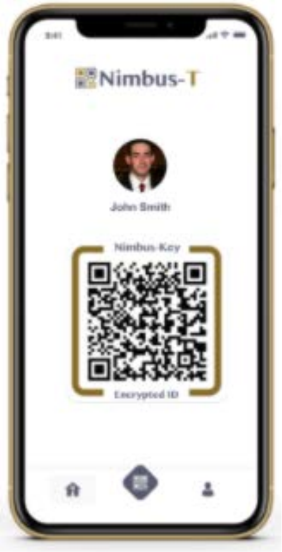


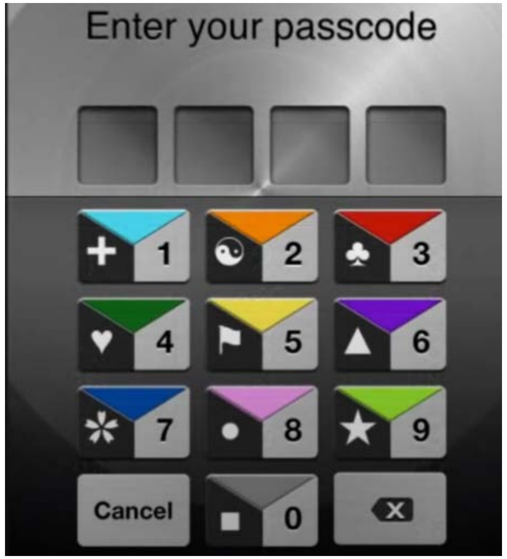
KB4-CON
2019

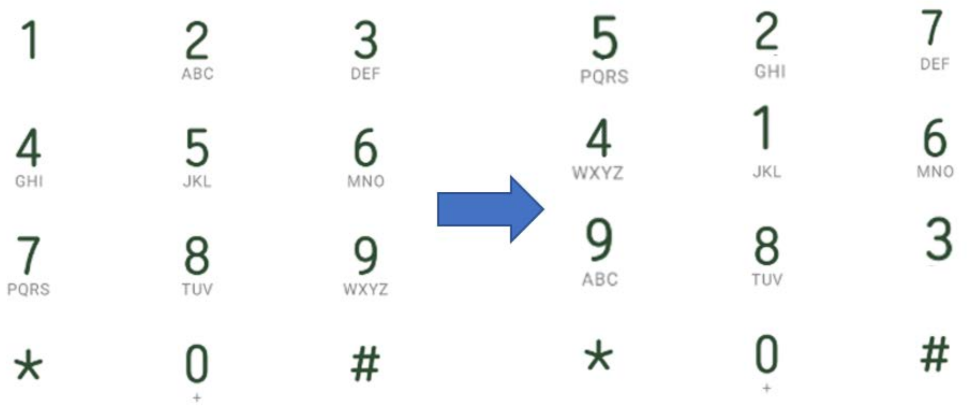
Types of MFA

<u>Additional Sub-Popular Examples</u>

- QR codes and logins
- Multi-character PIN keypads
- Move around PIN keypad each login



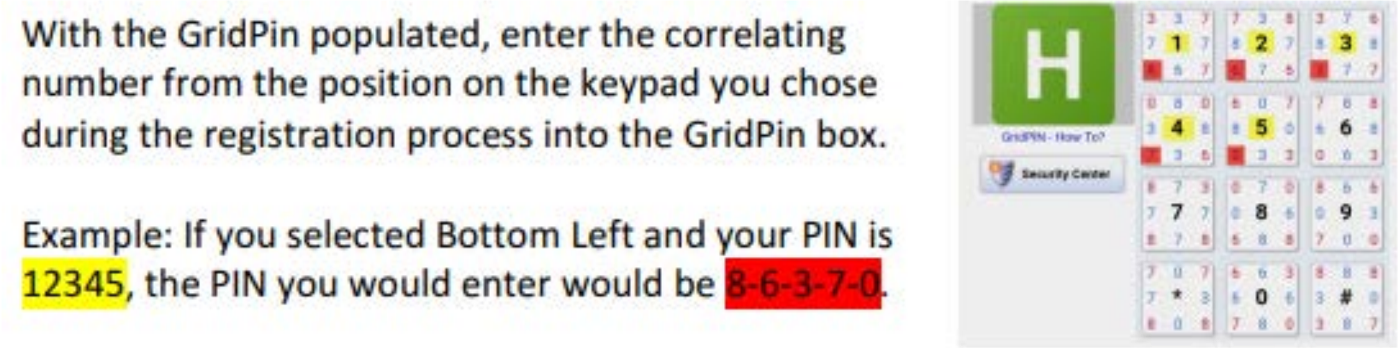




Types of MFA

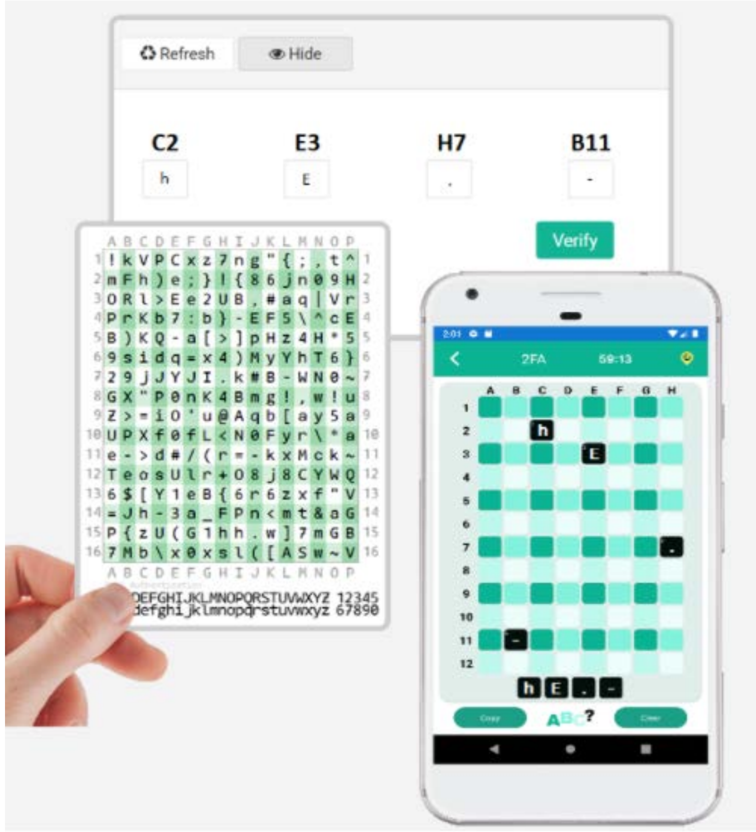
More Something You Know Examples

- Code lookup sheets
- Solve math problems



With the GridPin populated, enter the correlating number from the position on the keypad you chose during the registration process into the GridPin box.

Example: If you selected Bottom Left and your PIN is 12345, the PIN you would enter would be 8-6-3-7-0.



Agenda

- General Types of MFA
- How to Hack MFA
- The Good, the Bad, and the Ugly
- How to Pick the Right MFA Solution

Hacking MFA

Lots of Specific Hacking Examples If You Want More After This Webinar

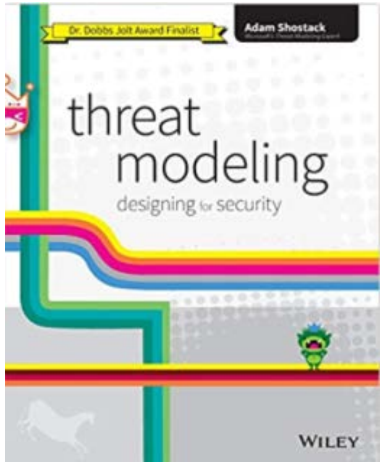
- **Many Ways to Hack MFA webinar**
  - 12-18 hacking examples depending on which version you view
  - https://info.knowbe4.com/webinar-12-ways-to-defeat-mfa
- **12 Ways to Hack 2FA eBook** (free)
  - 18-ways to hack various MFA solutions
  - https://info.knowbe4.com/12-way-to-hack-two-factor-authentication
- **Hacking Multifactor Authentication** book (Wiley)
  - https://www.amazon.com/Hacking-Multifactor-Authentication-Roger-Grimes/dp/1119650798
  - 50+ examples of MFA hacking examples

Hacking MFA

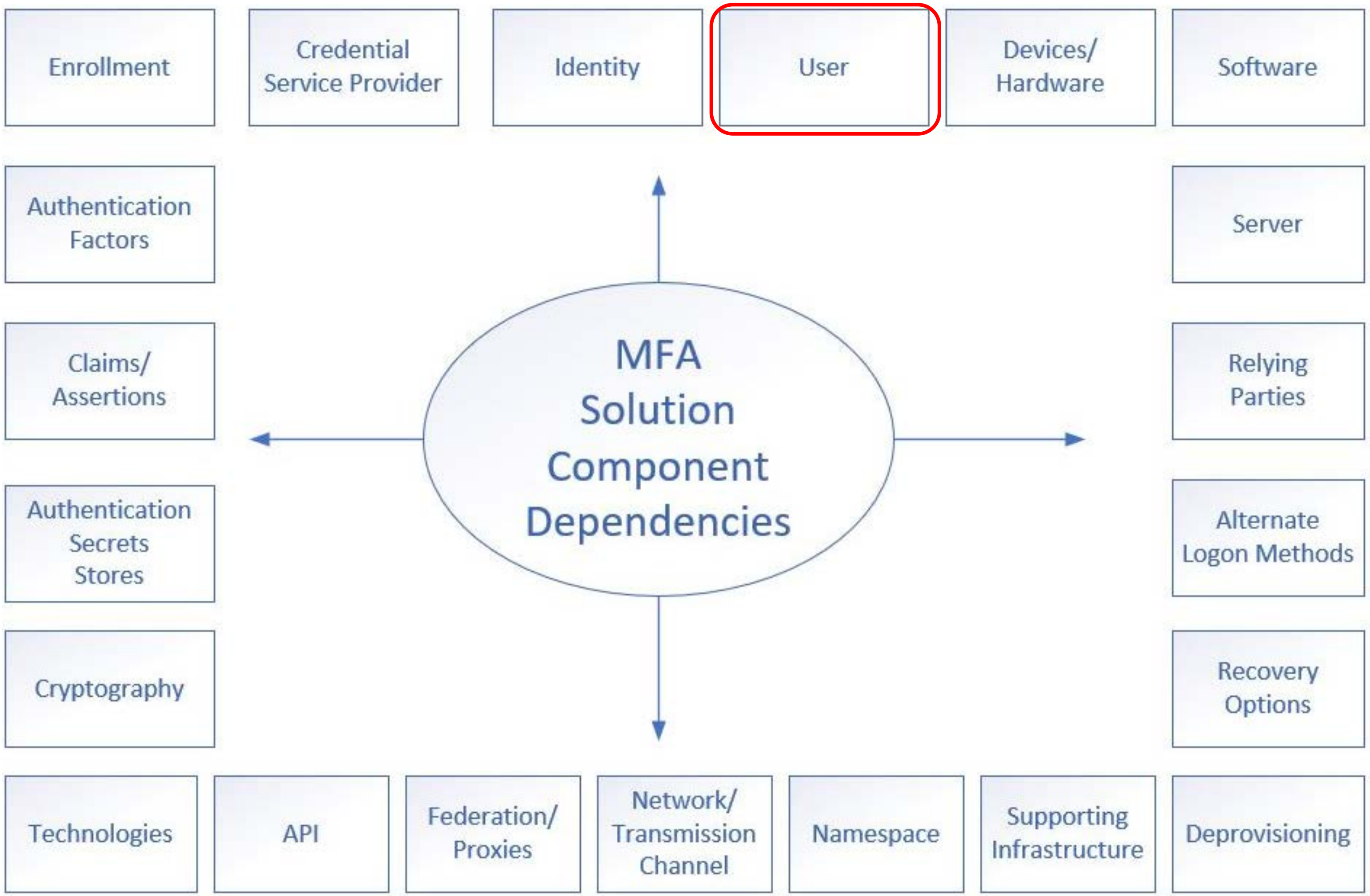
General Threat Modeling Methodology

- Document involved dependencies and components
- Brainstorm different possible attacks against each
- Test attacks

- I’m a fan of **Threat Modeling: Designing for Security**
- https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998
- Older, expensive, any threat modeling book will do



Hacking MFA



Enrollment

Credential Service Provider

Identity

User

Devices/ Hardware

Software

Authentication Factors

Server

Claims/ Assertions

MFA Solution Component Dependencies

Relying Parties

Authentication Secrets Stores

Alternate Logon Methods

Cryptography

Recovery Options

Technologies

API

Federation/ Proxies

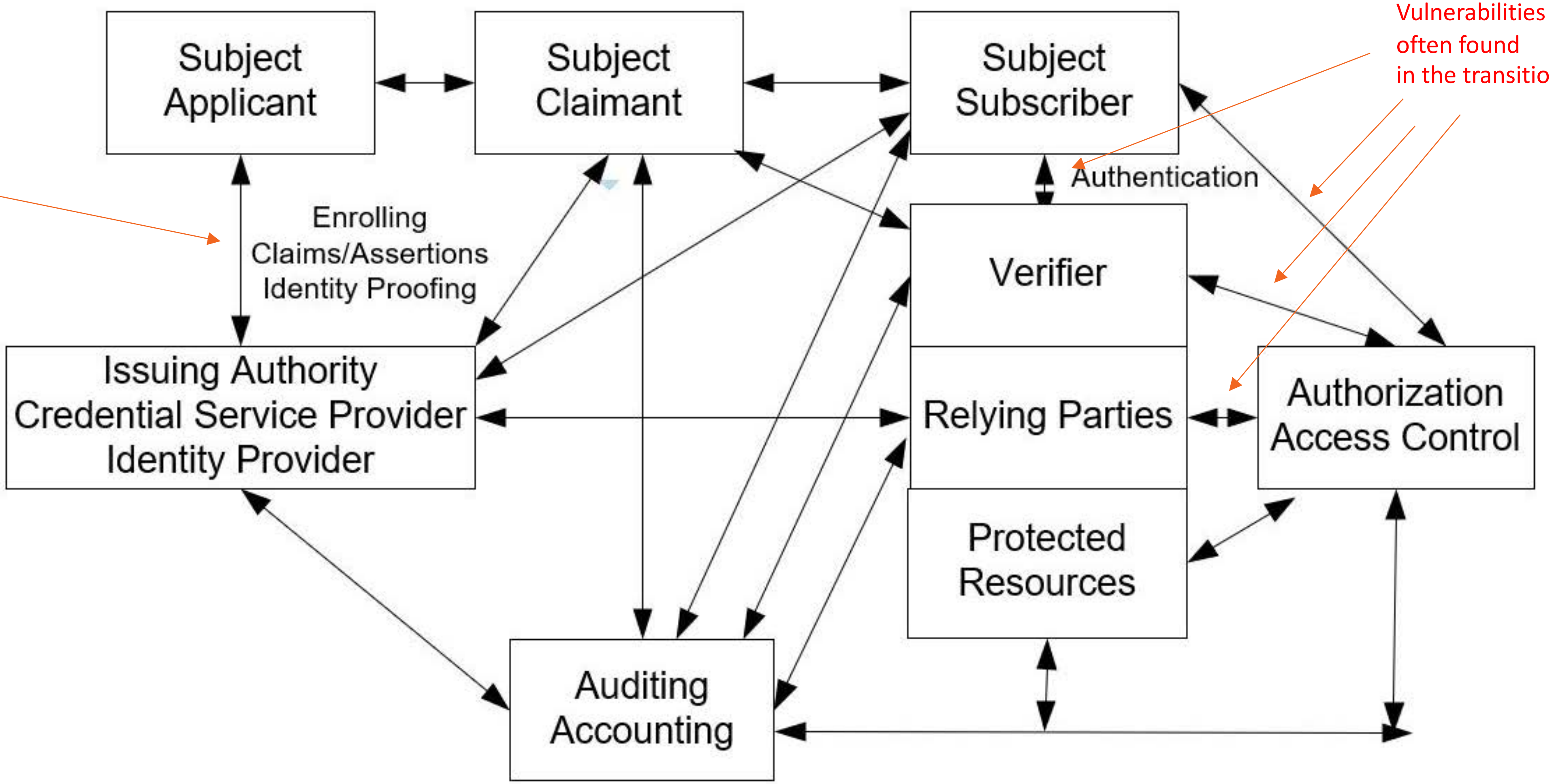
Network/ Transmission Channel

Namespace

Supporting Infrastructure

Deprovisioning

Hacking MFA



Vulnerabilities often found in the transitions

Vulnerabilities often found in the transitions

Hacking MFA

Hacking Methodology

Basic attack methods that work against most MFA solutions

- Social Engineering (most popular)
- Exploit Programming bug
- Weak verification between components
- Eavesdropping/MitM
- Alternate recovery/bypass
- Weak default configuration settings
- Data/Network traffic malformation
- 3rd Party Reliance issue (e.g. DNS, Active Directory, etc.)
- Physical attack
- Other

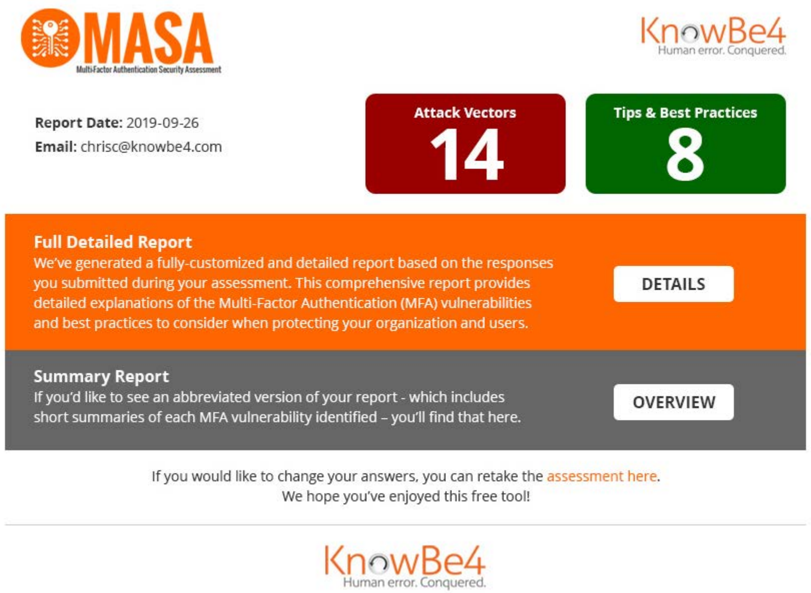
Hacking MFA

Let Me Threat Model Your MFA Solution

KnowBe4 **Multifactor Authentication Security Assessment** (MASA) tool

https://www.knowbe4.com/multi-factor-authentication-security-assessment

- Asks you a series of questions and then tells you how I could hack it



Report Date: 2019-09-26
Email: chrisc@knowbe4.com

Full Detailed Report
We've generated a fully-customized and detailed report based on the responses you submitted during your assessment. This comprehensive report provides detailed explanations of the Multi-Factor Authentication (MFA) vulnerabilities and best practices to consider when protecting your organization and users.

Summary Report
If you'd like to see an abbreviated version of your report - which includes short summaries of each MFA vulnerability identified – you'll find that here.

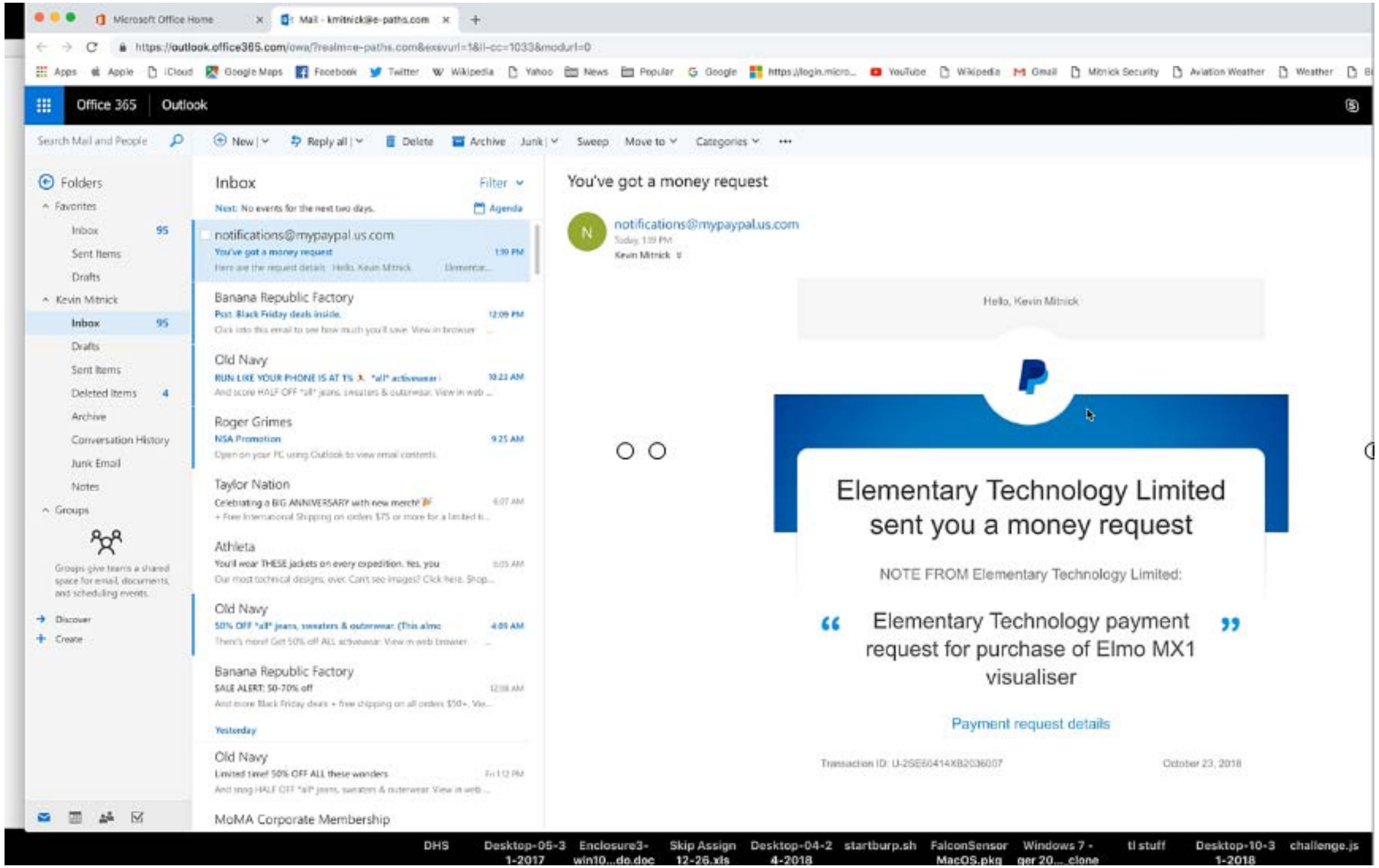
If you would like to change your answers, you can retake the assessment here.
We hope you've enjoyed this free tool!

Hacking MFA

<u>Hacking Demo</u>

Kevin Mitnick

- Simulated PayPal phishing attack



Inbox

Next: No events for the next two days.

notifications@mypaypal.us.com
You've got a money request — 1:39 PM
Here are the request details Hello, Kevin Mitnick Elementar...

Banana Republic Factory
Psst. Black Friday deals inside. — 12:09 PM
Click into this email to see how much you'll save. View in browser

Old Navy
RUN LIKE YOUR PHONE IS AT 1% *all* activewear — 10:23 AM
And score HALF OFF *all* jeans, sweaters & outerwear. View in web ...

Roger Grimes
NSA Promotion — 9:25 AM
Open on your PC using Outlook to view email contents.

Taylor Nation
Celebrating a BIG ANNIVERSARY with new merch! — 6:07 AM
+ Free International Shipping on orders $75 or more for a limited ti...

Athleta
You'll wear THESE jackets on every expedition. Yes, you — 5:05 AM
Our most technical designs, ever. Can't see images? Click here. Shop...

Old Navy
50% OFF *all* jeans, sweaters & outerwear. (This alme — 4:05 AM
There's more! Get 50% off ALL activewear. View in web browser

Banana Republic Factory
SALE ALERT: 50-70% off — 12:08 AM
And more Black Friday deals + free shipping on all orders $50+. Vie...

Yesterday

Old Navy
Limited time! 50% OFF ALL these wonders — Fri 1:12 PM
And snag HALF OFF *all* jeans, sweaters & outerwear. View in web ...

MoMA Corporate Membership

Groups give teams a shared space for email, documents, and scheduling events.

You've got a money request

notifications@mypaypal.us.com
Today, 1:39 PM
Kevin Mitnick

Hello, Kevin Mitnick

Elementary Technology Limited sent you a money request

NOTE FROM Elementary Technology Limited:

“Elementary Technology payment request for purchase of Elmo MX1 visualiser”

Payment request details

Transaction ID: U-2SE60414XB2036007 — October 23, 2018

Hacking MFA

Hacking Demo - Kevin Mitnick - Simulated PayPal phishing attack

1. Phishing email contained URL to 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

Hacking MFA

Hacking Methods Common to All MFA Solutions

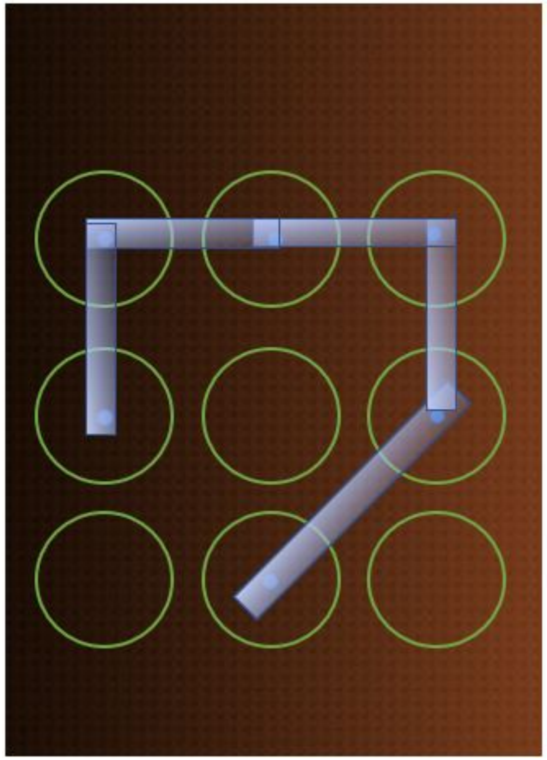
- Social engineering
- Man-in-the-Middle Attacks (90% of MFA solutions)
- Fake web sites where successful authentication was faked
- Recovery/alternate methods
- Namespace attacks
- Programming bugs
- Physical attacks (hardware MFA)
- Cold boot memory attacks (doesn’t work on split-key methods)
- Any attack method not involving authentication (e.g. unpatched software)

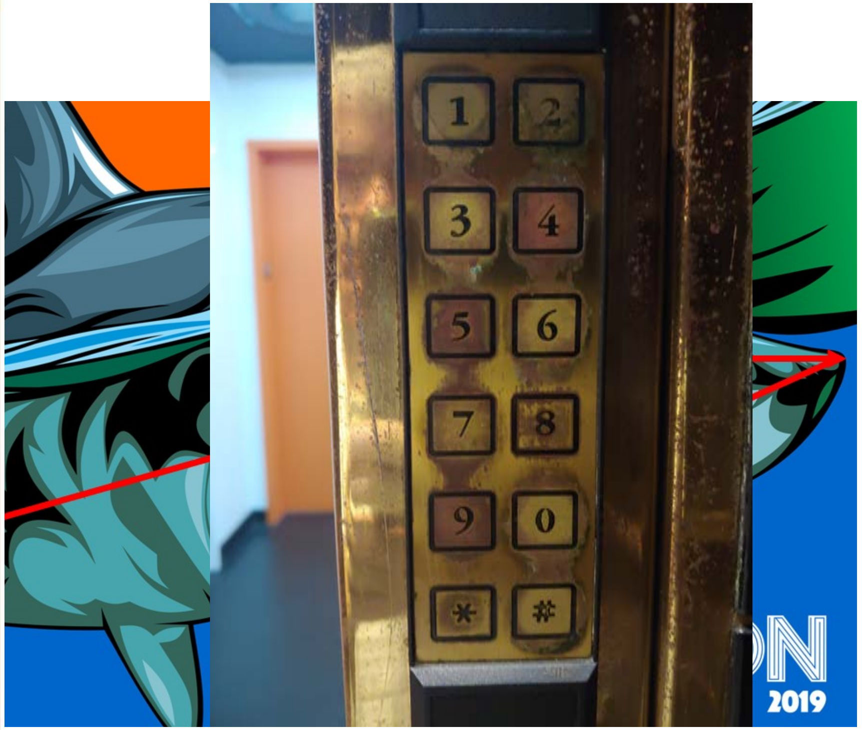
Hacking MFA

<u>Specific MFA Hacking Methods</u>

Per MFA Type – Picture-based

- Shoulder surfing
  - Pattern can often be seen or memorized from far away even with awkward angles
  - Certain picture attributes are more commonly used for selections
- Image could be duped and fake used to capture movements
- Surface clues left behind



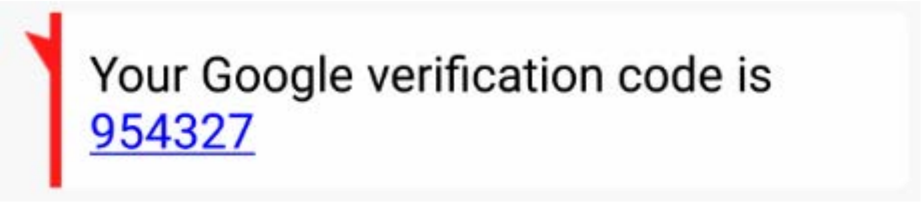


Hacking MFA

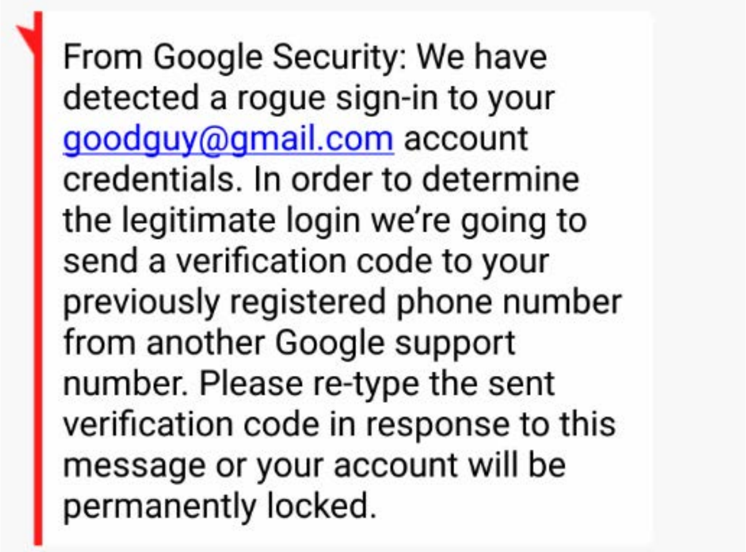
<u>Common Specific MFA Hacking Methods</u>

Per MFA Type – SMS-based

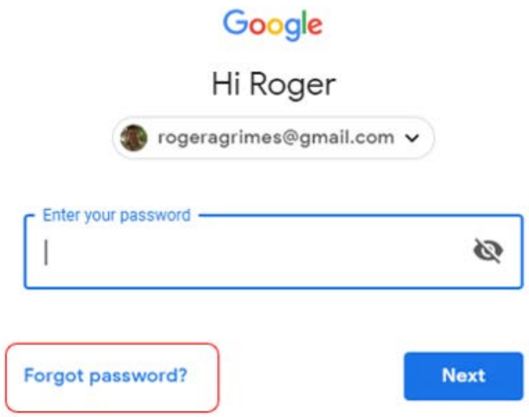
- SIM Swapping Attacks
- Fake SMS recovery methods

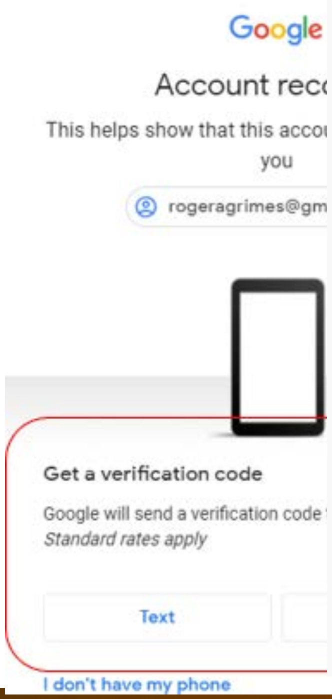


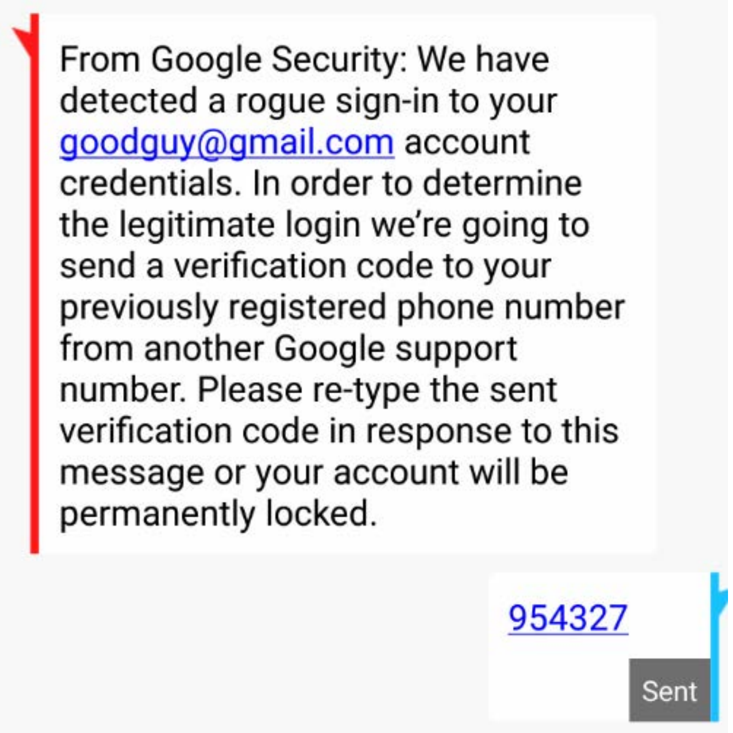
Your Google verification code is 954327



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.







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

Sent

Hacking MFA

Specific MFA Hacking Methods

Per MFA Type – Phone Voice-based

- No authentication other than voice or phone number which can be spoofed
- “Hi, I’m from”
  - Microsoft
  - Your bank
  - Your credit card company
  - Your airline company
  - Your hotel company
  - PayPal
  - IRS, law enforcement, etc.

Hacking MFA

Specific MFA Hacking Methods

Per MFA Type – Phone App-based

- MitM attacks can still work in many cases

Hacking MFA

Specific MFA Hacking Methods

Per MFA Type – Biometrics

- Stolen biometrics
- Mimicked biometrics
- Inaccurate biometrics

Hacking MFA

Specific MFA Hacking Methods

Per MFA Type – OTP/TOTP

- MitM attacks still work (90% of cases)
- No/poor rate limits for PIN inputs
- Stolen seed values allow duplicate instances to be created
- Bad non-standard crypto
- Non-expiring vacation/recovery codes
- Physical attacks

Agenda

- General Types of MFA
- How to Hack MFA
- The Good, the Bad, and the Ugly
- How to Pick the Right MFA Solution

KnowBe4
Human error. Conquered.

Good, Bad, and Ugly

- All MFA can be hacked
- But some are better than others

Good, Bad, and Ugly

Not Considered Strong

- Picture/pattern-solving solutions
- SMS-based MFA
  - US gov't has been saying to avoid since 2017 (NIST SP 800-63)
- 1FA token solutions
- 1FA biometrics
  - Especially for remote logons
- Overly complex solutions
  - Too strong

Good, Bad, and Ugly

Crypto Considerations

- Only use MFA solutions that use known, generally accepted cryptography and key sizes
- Start to think about crypto-agility and quantum-resistant crypto

- Run away from MFA solutions with proprietary or secret cryptography
  - Make sure MFA solution uses standard, open, cryptography
  - If the vendor won't show you their cryptography algorithms, do not use their solution
  - Good crypto is very, very, very hard to create

Good, Bad, and Ugly

Like

- Phone apps good
- Phone apps with push notification ability even better
- Multifactor FIDO2 (Fast Identity Online standard) is fairly strong
- Look for OATH (not OAUTH) hardware tokens
- Look for biometric vendors that protect/obscure/hash your stored biometric traits, so that having a stolen biometric attribute database is not enough to compromise your biometric traits forever
- Look for vendors with anti-replay defenses
- Look for vendors with large groups of customers and staying power
- Look for vendors who prioritize bug fixes and have open bug bounties

Good, Bad, and Ugly

Love

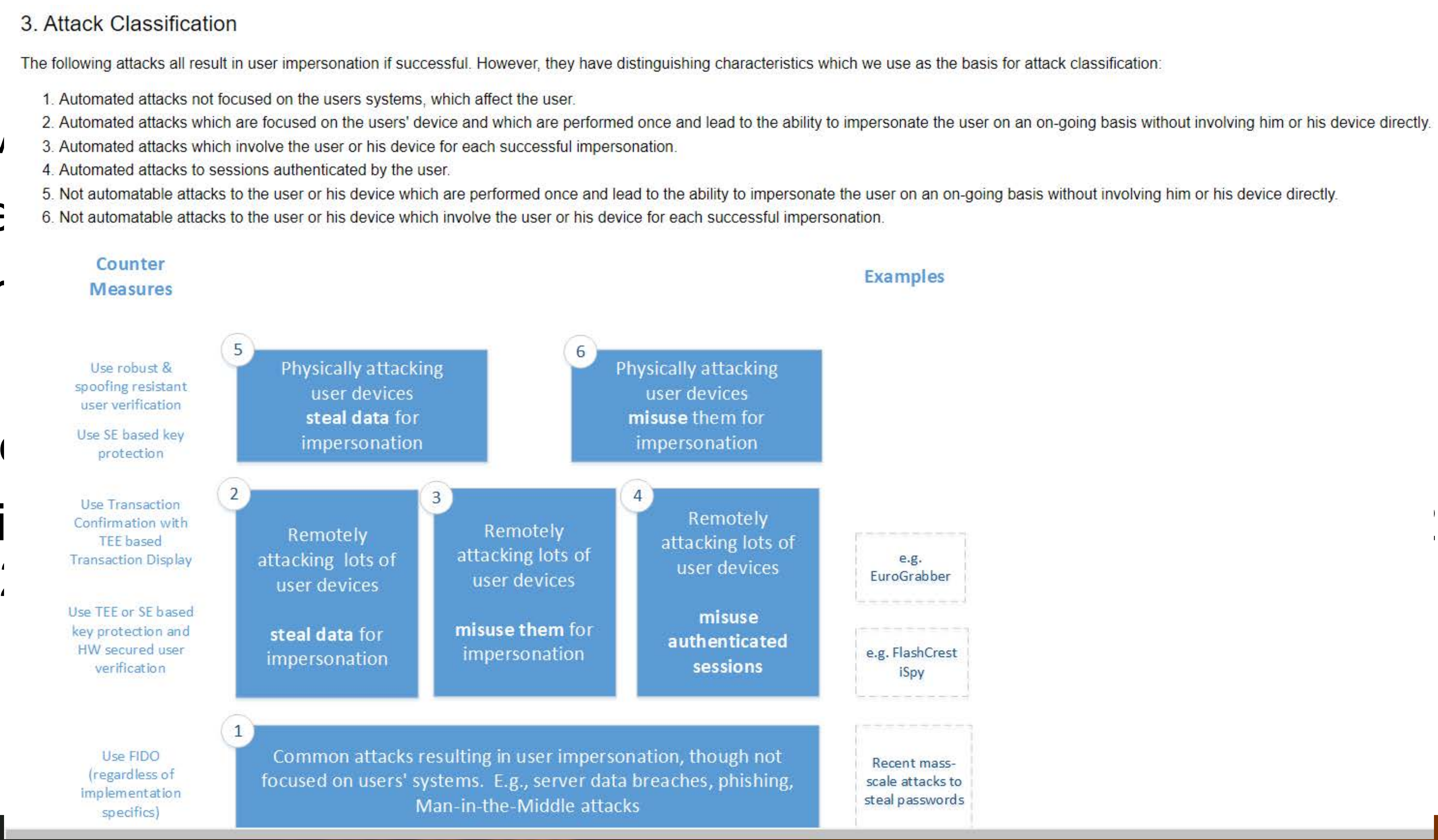
- LOVE MFA vendors who share their threat modeling, like FIDO2
- Fast Identity Online (FIDO), fidoalliance.org
- Standard, not a vendor

- FIDO Security Reference document
- https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html

Good, Bad, and Ugly

Love

- LOVE M
- Fast Ide
- Standar
- FIDO S
- https://fi .0-id-
  201802



3. Attack Classification

The following attacks all result in user impersonation if successful. However, they have distinguishing characteristics which we use as the basis for attack classification:

1. Automated attacks not focused on the users systems, which affect the user.
2. Automated attacks which are focused on the users' device and which are performed once and lead to the ability to impersonate the user on an on-going basis without involving him or his device directly.
3. Automated attacks which involve the user or his device for each successful impersonation.
4. Automated attacks to sessions authenticated by the user.
5. Not automatable attacks to the user or his device which are performed once and lead to the ability to impersonate the user on an on-going basis without involving him or his device directly.
6. Not automatable attacks to the user or his device which involve the user or his device for each successful impersonation.

Counter Measures

Examples

Use robust & spoofing resistant user verification

Use SE based key protection

5 Physically attacking user devices **steal data** for impersonation

6 Physically attacking user devices **misuse** them for impersonation

Use Transaction Confirmation with TEE based Transaction Display

Use TEE or SE based key protection and HW secured user verification

2 Remotely attacking lots of user devices **steal data** for impersonation

3 Remotely attacking lots of user devices **misuse them** for impersonation

4 Remotely attacking lots of user devices **misuse authenticated sessions**

e.g. EuroGrabber

e.g. FlashCrest iSpy

Use FIDO (regardless of implementation specifics)

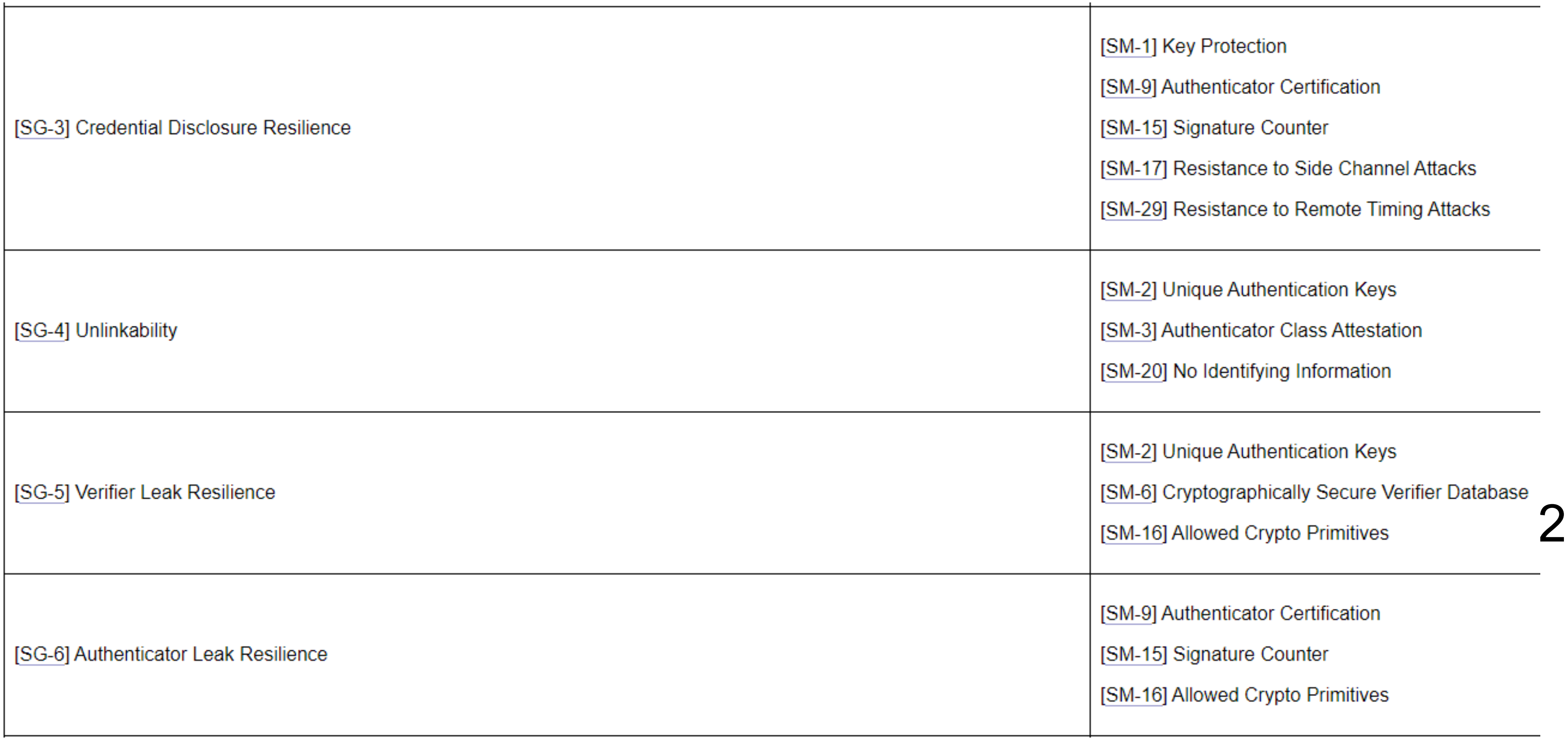
1 Common attacks resulting in user impersonation, though not focused on users' systems. E.g., server data breaches, phishing, Man-in-the-Middle attacks

Recent mass-scale attacks to steal passwords

Good, Bad, and Ugly

Love

- LC
- Fa
- Sta
- FI
- htt 2.0-id-
20



[SG-3] Credential Disclosure Resilience	[SM-1] Key Protection [SM-9] Authenticator Certification [SM-15] Signature Counter [SM-17] Resistance to Side Channel Attacks [SM-29] Resistance to Remote Timing Attacks
[SG-4] Unlinkability	[SM-2] Unique Authentication Keys [SM-3] Authenticator Class Attestation [SM-20] No Identifying Information
[SG-5] Verifier Leak Resilience	[SM-2] Unique Authentication Keys [SM-6] Cryptographically Secure Verifier Database [SM-16] Allowed Crypto Primitives
[SG-6] Authenticator Leak Resilience	[SM-9] Authenticator Certification [SM-15] Signature Counter [SM-16] Allowed Crypto Primitives

Good, Bad, and Ugly

Love

LOVE MFA vendors who:

- Share their threat modeling
- Practice SDL and tell you how they do it
- Use open bug bounties
- Use open standards
- Do regular pen testing of their solution using external vendors
- Open and transparent
- Don’t try to claim they are “unhackable”

Good, Bad, and Ugly

General

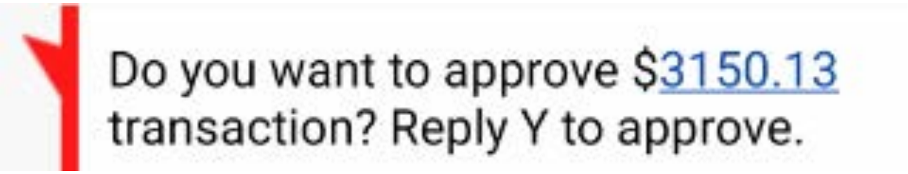
- Make sure MFA developers use security development lifecycle (SDL) techniques and tools
- Make sure any PIN inputs have rate-limiting/throttling/account lockout features enabled
- All “secrets” used to generate initial MFA values and logon values should have expiration periods
- Tying MFA solution to particular devices and websites/services prevents MitM attacks

Good, Bad, and Ugly

Transaction-Based MFA

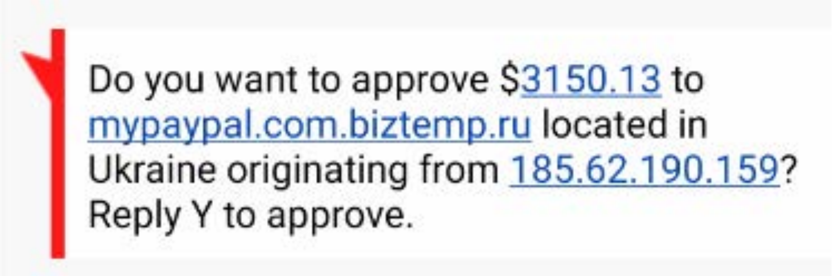
- Use MFA that gives you enough details to make an intelligent, low-risk, decision

Normal confirmation message



Do you want to approve $3150.13 transaction? Reply Y to approve.

Better confirmation message

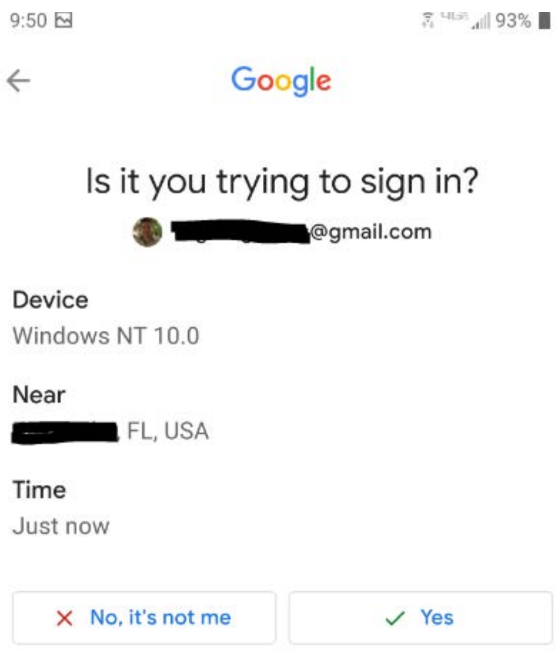


Do you want to approve $3150.13 to mypaypal.com.biztemp.ru located in Ukraine originating from 185.62.190.159? Reply Y to approve.

Good, Bad, and Ugly

Transaction-Based MFA

- Does that push notification message below include enough detail?



9:50 93%

Google

Is it you trying to sign in?

[redacted]@gmail.com

Device
Windows NT 10.0

Near
[redacted] FL, USA

Time
Just now

Maybe. Yes, for most attacks. Maybe not for an intelligent MitM replay-attack. IP address, browser type, and other details would be even better

I get weird locations when using VPNs sometimes, teaching me to ignore location prompt

Good, Bad, and Ugly

Parting Thoughts

- No matter which type of MFA you choose, educate everyone about the common possible attacks
  - You wouldn't give people passwords without warning them about common hacker tricks

Other Lessons Learned

- Stronger is not necessarily better
- Most admins/users are not overly accepting of novel, new, MFA methods, even if better and stronger
- If MFA solution is too hard, it won’t get much traction
- Every MFA solution has trade offs
- All can be hacked, but most of the time still decreases significant risk

Other Lessons Learned

Conditional Access

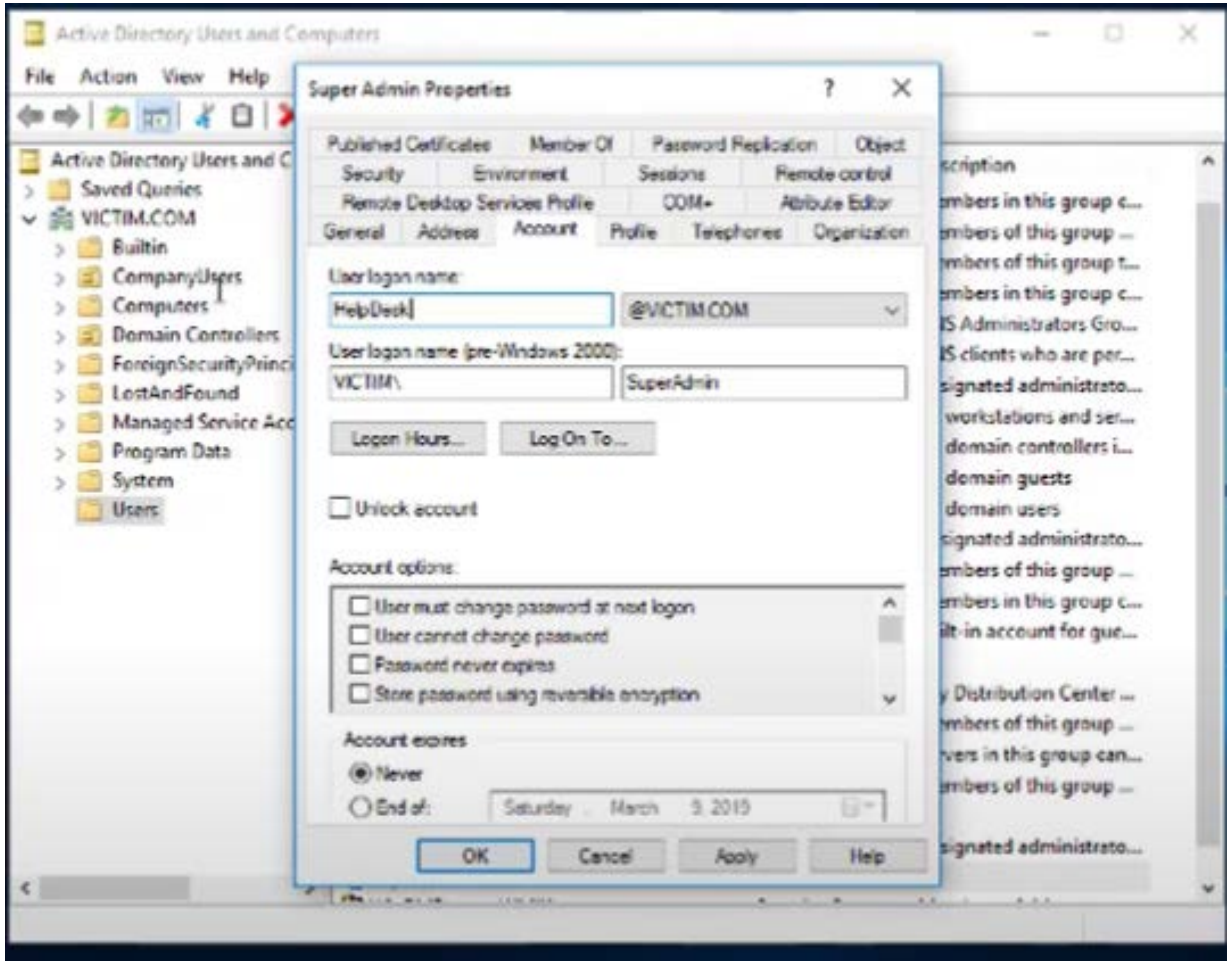
- Many MFA solutions use “conditional access” to add to what is evaluated during authentication
- Example: User must be in ‘HR group”, must be using previously registered device, and put in the correct logon name, and use valid TOTP
- Conditional access can be used to stop some advanced attack methods

- Important!: Conditional access attributes used to evaluate authentication must be protected like they were passwords

Other Lessons Learned

Conditional Access Attack Example

- Smartcards and Active Directory demo
- https://www.youtube.com/watch?v=OLQ3IAMuokI
- In it, I change the admin's email address to Help Desk and it makes Help Desk user admin
- This type of attack is never looked for, difficult to detect and stop


Super Admin Properties

User logon name: HelpDesk @VICTIM.COM

User logon name (pre-Windows 2000): VICTIM\ SuperAdmin

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Saturday , March 9, 2019

Agenda

- General Types of MFA
- How to Hack MFA
- The Good, the Bad, and the Ugly
- How to Pick the Right MFA Solution

Picking the Right MFA Solution

Steps to Pick the Right MFA Solution For You

1. Create a project team
2. Create a project plan
3. Educate
4. Determine what needs to be protected
5. Choose required and desired features
6. Research/select vendor solutions
7. Conduct a pilot project
8. Select a winner
9. Deploy to production

Picking the Right MFA Solution

Steps to Pick the Right MFA Solution For You

- **What do you want to protect?**
  - No MFA solution protects everything
  - Make a list of your critical apps that you must protect and see which MFA solutions can protect them
  - Apps, OS's, device types, clouds, etc.
- **Is there a solution type that natural fits better in your company?**
  - Some companies are more open to tokens, phone-based, or biometrics

- Every vendor and question to ask in spreadsheet form:
  wiley.com/go/hackingmultifactor

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

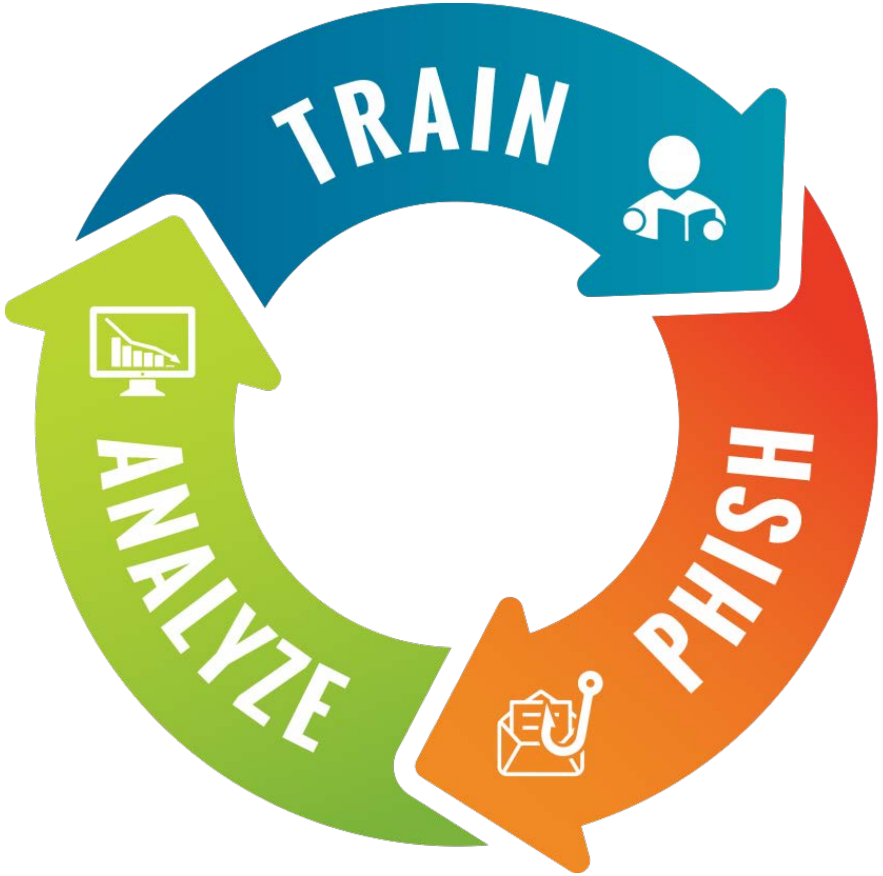
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

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!

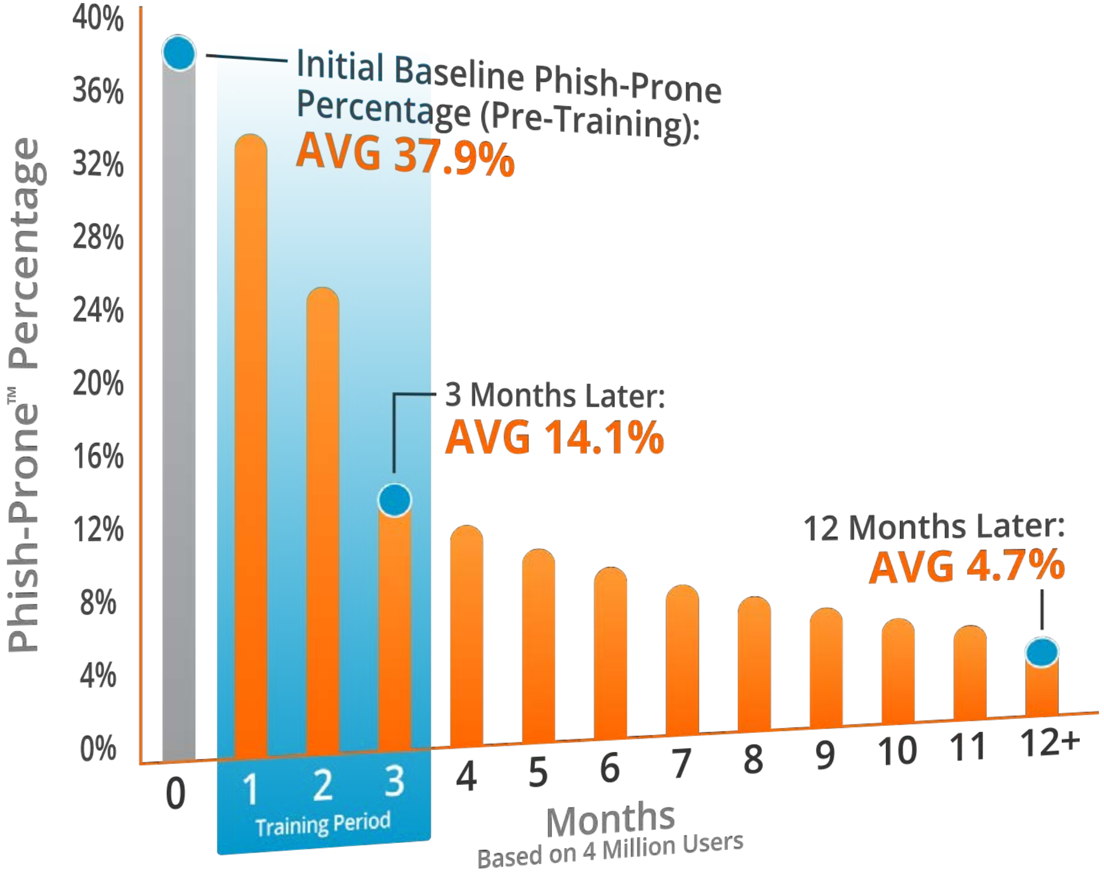


Generating Industry-Leading Results and ROI

- 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://www.linkedin.com/in/rogeragrimes/

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