How to Implement a Successful Multi-Factor Authentication Strategy

Presented by
Chris Hacker & Steve Hargraves

February 20th, 2020

FNF FAMILY OF COMPANIES

ShortTrack

AMERICAN LAND TITLE ASSOCIATION

Meet Our Presenters

Chris Hacker

Co-Founder & CTO

chris@shorttrack.io

Steve Hargraves

Co-Founder & COO

steve@shorttrack.io

ShortTrack

Agenda

Multi-Factor Authentication

- Why you should use multi-factor authentication
- Tips to choose the right solution for your company
- How to implement multi-factor authentication
- Best practices to ensure workflow efficiency
- Is this security measure enough?

Why you should use multi-factor authentication

Why Multi-Factor?

> “The days of fixing this with a firewall or IT patch are over. This is an arms race...”

—Dr. Barbara Endicott-Popovsky, Executive Director, Center for Information Assurance and Cybersecurity, University of Washington

Why Multi-Factor?

- Identity theft is an easy, low-risk, high-reward
- Weak or stolen user credentials - credential stuffing.
- Keylogging, phishing, pharming, brute force, and MITM.
- More than stealing data.

  Destroy data.

  Change programs or services

  Holding data hostage

  Transmit propaganda, spam, or malicious code.

Why Multi-Factor?

Passwords Are No Longer Enough

- Passwords are responsible for **81%** of attacks.
- Complex passwords are hard to remember
- Often used across multiple sites.
- Users tend to write them down
- Common words with easily discoverable information

password1

Daisy042382

Why Multi-Factor?

Key Hacking Statistics

Headlines tend to belong to the large household-name companies, but…

Phishing attacks considered to be one of the top IT security threats.

Large integrated health care system self study of 15,964 mock phishing emails.

31% Businesses with < 250 employees

15% Employees will click the link

4% Employees surrender their credentials

Why Multi-Factor?

ALTA Best Practice Pillar 3

American Land Title Association
Protecting the American Dream Since 1907

Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.

November 21, 2019 procedures update:

Utilize multifactor authentication for all remotely-hosted or remotely accessible systems storing, transmitting or transferring Non-public Personal Information.

Why Multi-Factor?

CyberSecurity Challenges

User credentials vulnerable to phishing attacks

Hackers use stolen credentials to access the network

NPI and other sensitive data exposed

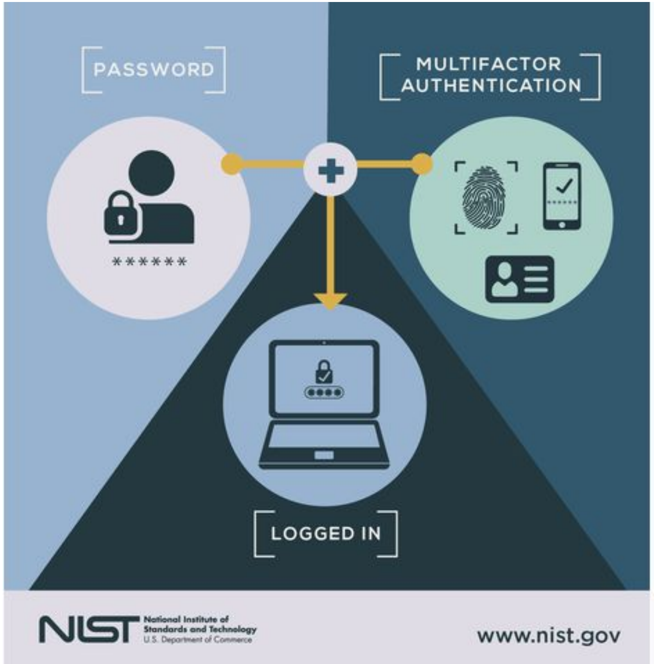
Why Multi-Factor?

MFA, also known as two-factor authentication (2FA), credentials fall into three categories:

1. **Something you know:** passwords, PINs, combinations, code words, etc.

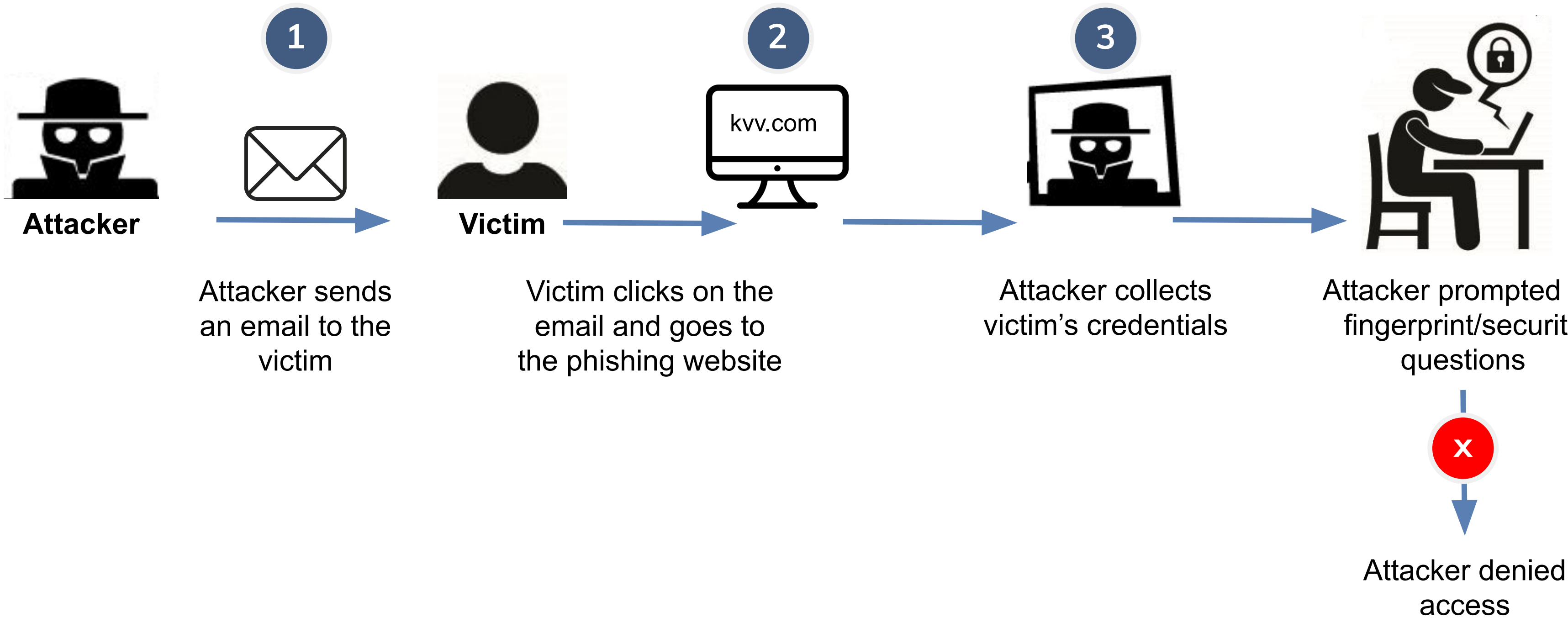
2. **Something you have:** computer, phone, keys, USB drives and token devices.

3. **Something that you are:** fingerprints, palm scanning, facial recognition, retina scans, iris scans and voice verification.


PASSWORD
******
MULTIFACTOR AUTHENTICATION
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

Why Multi-Factor?

How MFA combats common cyber attacks



Attacker sends an email to the victim

Victim clicks on the email and goes to the phishing website

Attacker collects victim’s credentials

Attacker prompted for fingerprint/security questions

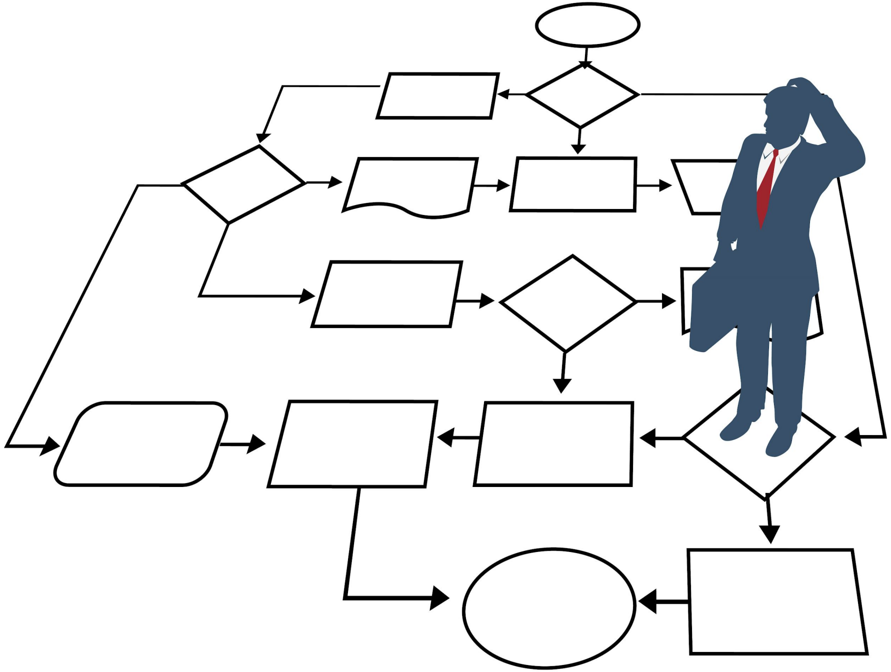
Attacker denied access

Tips to choose the right solution for your company

Tips to choosing the right solution

Key Attributes:

- Easy to Deploy
- Easy to Use
- Easy to Manage



Tips to choosing the right solution

Bank of America
citi
WELLS FARGO
JPMorganChase

Consider the following questions:

Microsoft Azure
aws
op2
Office 365
Apple ID

- Where do I already have access to a solution?
- Does the solution provide a range of options for all of your uses?
- Does it offer the flexibility to add new authentication methods?
- Does it enable you to support user choice and emergency access requirements?
- Do you need adaptive MFA?

Tips to choosing the right solution

Adaptive MFA

- Require a user to use certain factors to authenticate based on how the user is logging in.
  - New mobile phone? Different location than usual?
- Improves the experience of the user
  - only asked for an additional factor when necessary.

How to implement multi-factor authentication

How To Implement MFA

- Campaign & train
- Start with admin accounts
- Plan for wider deployment
- Make MFA easier on employees
- Have a support plan
- Measure & monitor

How To Implement MFA

Campaign & Train

- Sell it internally: Run an effective internal communications campaign
    - Makes it clear to users what they need to do and, more importantly, why
    - Avoids them seeing MFA as a nuisance or as ‘big brother’ company tracking.
- Focus on awareness
    - Emails, posters in break room, banners in hallways
    - What they need to do & where to find documentation and support
- Provide Support
    - FAQ’s & Training videos
    - Training sessions

How To Implement MFA

Start with Admin Accounts

- Highest value and most urgent to secure targets
    - Tend to be more savvy
    - Opportunity to identify and remove unnecessary privileges
- Target key business roles that would have a major security impact
- Use lessons to plan a pilot deployment including users with different levels of access

How To Implement MFA

Plan for Wider Deployment

- Identify networks or systems that will require more work
  - SAML authentication
  - Legacy apps with out of date authentication, ie email (IMAP4, POP3, SMTP)
- Upgrade systems where possible to support MFA
- Restrict systems to local network only when upgrade isn’t possible
- Prepare to prioritize applications
- Add to new hire processes and require immediate setup

How To Implement MFA

Make MFA easier on Employees

- Consider the use cases and use biometrics, hardware keys, or apps on employee devices where possible.
    - If employees travel and have connectivity issues, consider apps that use OAUTH codes rather than push notifications.
    - Automated voice calls are preferable to SMS/texts.
- Offer choice of factors - not everyone wants to use biometrics.
- Include mobile devices with a Mobile Device Management solution.

How To Implement MFA

Have a Support Plan

- Have a plan to manage account lockouts
- Have a plan for lost devices
    - Easy and blame free so sessions and keys can be invalidated and recent activity audited
- Register more than one device where possible to eliminate downtime
    - Should be more annoying to use to prompt them to report primary device loss
- Automatically deprovision when employees change roles or leave

How To Implement MFA

Measure & Monitor

- Track security metrics for failed login attempts, blocked credential phishing, and denied privilege escalations.
- Continue MFA marketing during and after deployment
  - Collect feedback with polls and sessions
  - Start with the pilot group and expand with rollout
- Track helpdesk tickets, logs and turn times to monitor effects on productivity
- Test updates to confirm they don’t break MFA
- Test employees with phishing training and phishing your employees

Best practices to ensure workflow efficiency

Best Practices To Ensure Workflow Efficiency

- **Understand your requirements.**
- **Assess your applications.**
- **Choose factors and distribution tactics that fit your strategy.**
- **Take mobile security measures.**

Best Practices To Ensure Workflow Efficiency

Understand your requirements.

- Identify your purpose: For corporate access, to secure consumer-facing web portals, or both?
- Identify your organization’s processes and functionalities (use cases)
- Use the use cases to identify the applications you want to integrate with MFA.
  - All users, and
  - Across all cloud and on-premises applications, VPNs, endpoints and server logins, and
  - Required when users attempt to escalate privileges.

Best Practices To Ensure Workflow Efficiency

Understand your requirements.

- Purpose: For corporate access, to secure consumer-facing web portals, or both?
- Identify your organization’s processes and functionalities (use cases)
  - How do employees work together?
  - How do employees and consumers authenticate into applications?
  - Where and how is information accessed?
  - Where and how is your sensitive data accessed?
- Use the use cases to identify the applications you want to integrate with MFA.
  - All users, and
  - Across all cloud and on-premises applications, VPNs, endpoints and server logins, and
  - Required when users attempt to escalate privileges.

Best Practices To Ensure Workflow Efficiency

Assess your applications.

- **Consistent Authentication**: the more resources protected by the same user authentication experience, the lower cost and better experience you can provide.
- **Consider Single Sign-On (SSO) where possible**: Limit exposure and improve user experience by leveraging a portal to access applications and websites.

Best Practices To Ensure Workflow Efficiency

Choose factors and distribution tactics that fit your strategy.

- Many options for second authentication factor: hardware tokens, software tokens, security questions, SMS/text messages, biometrics, emails and phone calls.
- Consider what works best with the needs of your user population.
- **Distribution**: model and map your channels and use cases.

Best Practices To Ensure Workflow Efficiency

Take mobile security measures.

- Mobile devices are the new network perimeter.
- **Avoid SMS/text when possible**: Texts to a user's mobile phone can be socially engineered out of their control or compromised via device theft, SIM swapping or carrier account hijacking.
- **Consider alternatives with mobile devices**: push authentication or biometric capabilities.
- Encourage (require?) employees to lock their phones with fingerprint detection, set the time on password locks to 30 seconds or less, and enable remote wipe/remote recovery.

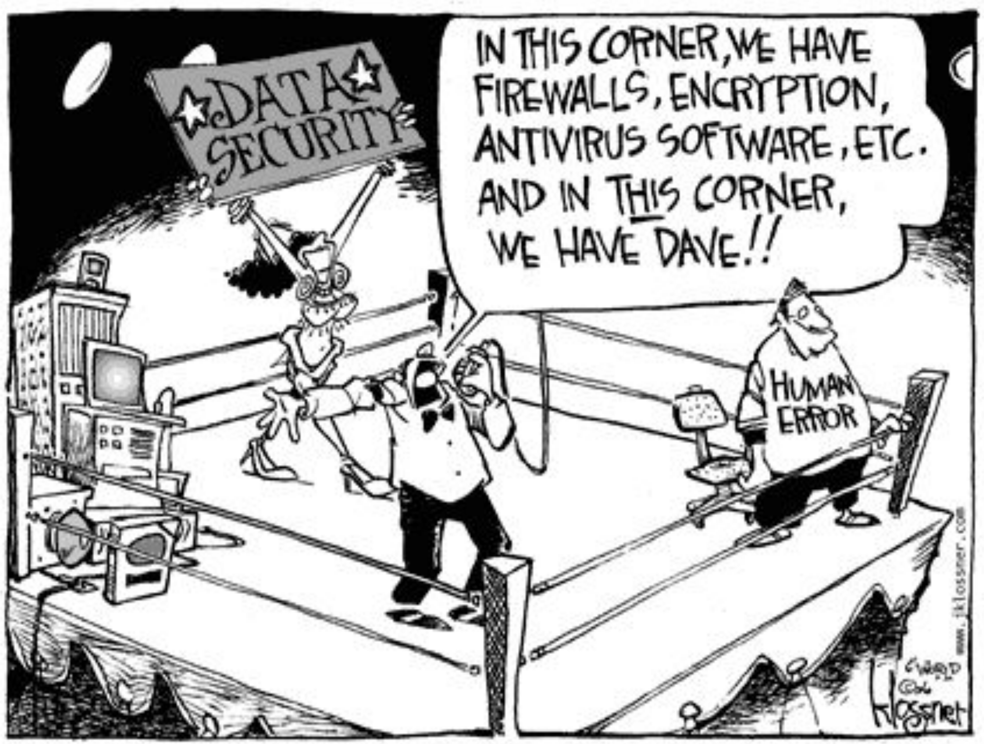
Best Practices To Ensure Workflow Efficiency

Lessons learned…

- **Implement MFA everywhere** – Partially deploying it in the organizations does very little good in protecting important applications and data.
- **Use adaptive MFA** – This will make for a better user experience and security.
- **Provide a choice of MFA methods** – By giving users several options to choose from, the user experience will be more positive for different user populations.
- **Combine MFA with SSO and least privilege access** – By combining multiple levels of security, the risk of compromised data is even lower.
- **Continuously re-evaluate MFA** – Verify that the deployment continues to meet the needs of the organization and its users. Make changes as necessary.
- Allow for emergency access options (e.g., if phone is dead)

Is this security measure enough?

Is MFA good enough?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Is MFA good enough?

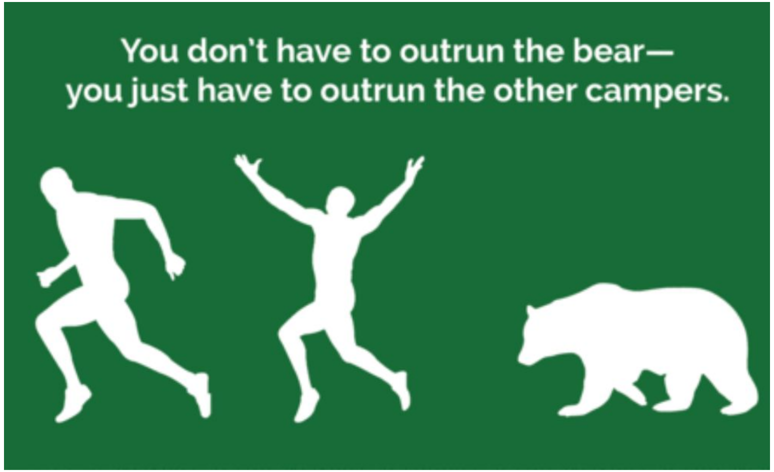
- Follow ALTA’s Pillar 3 Best Practices.
- Combine with other identity security solutions such as single sign-on (SSO) and least privilege access.
- Consolidate passwords with a password manager.
- Adopt a Social Media Policy. MFA is most often exploited through social engineering.
- Train, test, & re-train employees.

Is MFA good enough?

- No technology today will provide a 100% fail-safe system.

  BUT...

- MFA enhances the confidence of customers and consumers.
- MFA significantly raises the obstacles for would-be attackers.


You don't have to outrun the bear—
you just have to outrun the other campers.

Thank you!

American Land Title Association™
Protecting the American Dream Since 1907

FNF®
FAMILY OF COMPANIES

ShortTrack