Cybersecurity: The Increasing Need to Protect Our Devices

Brian Wallace, Founder & President, NowSourcing

Cybersecurity is needed now more than ever. Coronavirus has exposed why we're at risk. Large-scale growth of work-from-home technologies, customer-facing networks, online cloud services have all been exploited by cyber attackers. COVID-19 has led to increased susceptibility to attacks with a 30% increase in cyber attacks reported each week in March and April 2020 compared to pre-coronavirus.

Covid has taught us three important lessons: a cyberattack can spread faster than a biological virus, the economic impact of a digital shutdown could be immense, and recovering from digital destruction can be very challenging. Soon we could see cyber pandemics, a self-propagating, digital attack that exploits tech loopholes before patches and antivirus software become available, that can spread faster and further than a biological pandemic. Consequences of cyberattacks on devices include poor performance and bricked or inoperable devices. The consequences of cyberattacks on the world would be extremely costly.

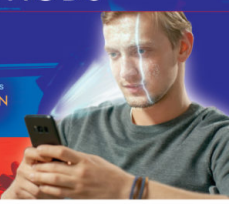
As we recover from the pandemic, businesses must re-evaluate their security policies and procedure to reflect the shift to remote work. Breaches will only increase until we **change our approach to authentication**. Authentication verifies that an individual is who they claim to be and confirms that person should be granted access. When your user authentication isn't secure, cybercriminals can bypass the system, taking whatever information they want.

Various authentication methods pose different strengths of security. Passwords and security questions are very weak.

Answers to security questions are often readily available online. Out-of-band voice is also weak because voice calls are easily intercepted or redirected. Time-based-one-time passwords are medium security. One-time codes expire after a short period, enhancing security, but are vulnerable to SIM hijacking, malware, and notification flooding attacks. Biometrics are high security; they are hard to fake, but, if the data is compromised, people can’t simply change their fingerprints or face. Legacy multi-factor authentication varies in security strength and depends on the weakest factor used. More factors don’t mean more security. Multi-factor authentication creates headaches for users, and lack of usability is likely to erode compliance with password best-practices, further compromising security.

Asymmetric cryptography leveraged by certificates is already universally trusted. Certificate-based authentication eliminates the need for passwords, reducing the change of user-error, phishing attacks, and hacked password databases. Multiple criteria are used to determine whether an attempt is invalid. The end-user granted easy access without remembering a password or needing a second device for authentication. This means extremely secure authentication that is also easier for everyone to use. Increased cybersecurity is imperative, making secure authentication methods a priority.

The Complete Guide to AUTHENTICATION METHODS



Hackers attack every 39 seconds

HOW DO WE REMAIN SECURE ONLINE?

AUTHENTICATION & Online Security

In 2018,

81% of security incidents *were tied to stolen, or weak passwords*

Breaches will only increase, until we change our approach to authentication

In 2019,

157,525 security incidents

3,950 confirmed data breaches

WHAT IS AUTHENTICATION & WHY IS IT IMPORTANT?

AUTHENTICATION

Verifies that an individual is who they claim to be

Confirms that person should be granted access

When your user authentication isn't secure, cybercriminals can bypass the system – taking whatever information they want

In 2020,

15 billion stolen credentials for sale on the dark web

AUTHENTICATION METHODS: Security & Convenience

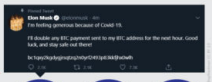
	SECURITY	Relies on a **"shared secret"** known to user and service provider
PASSWORDS & SECURITY QUESTIONS	Very Weak	Users responsible for protecting and remembering multiple passwords
		Answers to security questions are often readily available online
OUT-OF-BAND VOICE	Weak	Confirms identity by **calling a registered phone number**
		Voice calls are easily intercepted or redirected
		Requires user to have a second device and be available to answer call
TIME-BASED ONE-TIME PASSWORDS	Medium	**One-time code** sent through SMS, push notifications, or email
		Codes expire after a short period of time – enhancing security
		Vulnerable to SIM hijacking, malware, and notification flooding attacks
BIOMETRICS	High	**Hard to fake** – though some tech has issues with false positives
		No password to remember and no extra steps for end-user
		Only secure if biometric data is stored locally and protected by TPM/Enclave

The Problem WITH LEGACY MULTI-FACTOR AUTHENTICATION

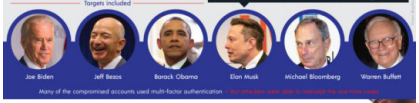
MULTI-FACTOR AUTHENTICATION (MFA)	SECURITY	Varies	**Requires two or more authentication methods** to login
			Most often combines a password and a one-time code
			Strength of security depends on the weakest factor used

In July 2020,

hackers took over the verified twitter accounts – offering to double their value if people sent them bitcoin



Targets included



Many of the compromised accounts used multi-factor authentication – but attackers were able to intercept the one-time codes

MORE FACTORS DOESN'T MEAN More Secure

Though widely used,

TWO-FACTOR AUTHENTICATION IS EASILY SPOOFED

- SMS authentication codes aren't encrypted and can be easily intercepted
- Encrypted instant messaging apps may send to multiple devices at once

BIOMETRICS CAN BE HIGHLY EFFECTIVE

BUT, IF THE DATA IS COMPROMISED,

people can't simply change their fingerprints or face

– making it a high-value target for attack

MORE FACTORS More Problems

Multi-factor authentication creates headaches for users

JUMPING BETWEEN DEVICES	REMEMBERING PASSWORDS	ACTING BEFORE ONE-TIME CODES EXPIRE
Username & password	Security questions	One-time codes

Most approaches still rely on a shared secret – which can be compromised by the user or an attack on the server

Lack of usability is likely to erode compliance with password best-practices – further compromising security

ASYMMETRIC CRYPTOGRAPHY

ASYMMETRIC CRYPTOGRAPHY IS ALREADY UNIVERSALLY TRUSTED

Used in TLS/HTTPS to secure trillions of dollars of transactions daily.

CERTIFICATES

A BETTER APPROACH TO *Authentication*

Certificate-based authentication eliminates the need for passwords – reducing the chance of user-error, phishing attacks, or hacked password databases

Utilizes multiple criteria to determine if an attempt is valid: user identity, device security posture, biometrics, IP address, and geolocation

End-user granted easy accesses without remembering a password or needing a second device for authentication

"There is no doubt that over time, people are going to rely less and less on passwords"

- **Bill Gates**
Co-founder of Microsoft

WE CAN HAVE IMMENSELY SECURE AUTHENTICATION THAT IS ALSO EASIER FOR EVERYONE TO USE

– Eliminating passwords is a reality today

Sources:
cvs.com/
blog/password-us
beyondidentity.com/technology
entrepreneur.com/article/309054
swoopnow.com/user-authentication
enterprise.verizon.com/resources/?page=1
pages.nist.gov/800-63-3/sp800-63b.html
searchsecurity.techtarget.com/definition/PKI
whatis.techtarget.com/definition/behavioral-biometrics
cnet.com/news/gates-predicts-death-of-the-password
okta.com/blog/2019/02/the-ultimate-authentication-playbook
theatlantic.com/sponsored/ibm-2016/beyond-passwords/1659
latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html
searchsecurity.techtarget.com/definition/one-time-password-OTP
wehavesecurity.com/2017/05/04/short-history-computer-password
searchsecurity.techtarget.com/definition/out-of-band-authentication
securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
threatstack.com/blog/what-is-pki-a-crash-course-on-public-key-infrastructure-pki
csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
allthingsauth.com/2018/02/27/sms-the-most-popular-and-least-secure-2fa-method
csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html
csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
forbes.com/sites/zakdoffman/2020/07/06/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime

Presented by:

BEYOND IDENTITY

NOWSOURCING

About the Author: *Brian Wallace is the Founder and President of NowSourcing, an industry leading infographic design agency in Louisville, KY and Cincinnati, OH which works with companies ranging from startups to Fortune 500s. Brian runs #LinkedInLocal events, hosts the Next Action Podcast, and has been named a Google Small Business Adviser for 2016-present. Follow Brian Wallace on LinkedIn as well as Twitter.*