Multi-Factor Authentication (MFA)

What is it? Why should I use it?

CYBERSECURITY

Tech Fair 2018

BOSTON UNIVERSITY

Recent Password Hacks

- **PlayStation Network (2011)**
  - 77 Million accounts hacked
- **Adobe (2013)**
  - 38 Million accounts hacked
- **Yahoo (2014)**
  - 3 Billion accounts hacked (that B is not a typo)
- **Under Armour (2018)**
  - 150 Million accounts hacked

What can I do?

- You can’t stop a data breach, but you can make your password less useful to hackers
- How? Use MFA if possible
- Even if someone gains access to your password, you might be protected

What is MFA?

- MFA (Multi-Factor Authentication)/ 2FA (Two-Factor Authentication)
- Uses multiple independent credentials
  - What you know
  - What you have
  - What you are
- Creates redundancy
  - One method fails, another to fall back on

Examples

- Log into website, receive one-time password via email or SMS
- Access VPN with password (e.g. vpn.bu.edu/2fa), answer prompt in DUO app on mobile device
- Access corporate network via USB device and password
- Enter high security facility with retina scan, and code

DUO etc.

- BU uses DUO to protect PII
- Many sites use SMS MFA
- Better option is to use app/ dedicated code generation device if possible

Downsides

- Inconvenient
  - Extra time to log in
  - Can’t log in without device (dead battery/ forgot)
- Can cause issues with applications depending on implementation

How to defeat MFA?

- Social Engineering
- Physical access to MFA security device
- Hacked Cookies
- Unknown methods

Summary

- Very important to use especially on critical accounts (Google, Apple)
  - Especially on accounts that are used for other MFA (email accounts etc.)
- Slight inconvenience is small price to pay for large increase in security
- Hackers go after the low-hanging fruit
- Go home and enable MFA on everything!

Questions?

BOSTON UNIVERSITY

Multi-Factor Authentication (MFA)

Why does it matter?

- Hacks happen all the time. We unfortunately cannot control how third parties store our sensitive data, but using MFA, we can make our passwords less useful to hackers.
- What if copies of your house key were entrusted to a third party to keep safe? Wouldn't you want to install another type of lock that only you could get through? This is a good (basic) analogy of MFA.
- Hackers usually go after the low hanging fruit. Don't be an easy target.

Largest hacks (> 50 million records)

Entity	Year	Records	Organization type	Method
Yahoo	2013	3,000,000,000	web	hacked
Yahoo	2014	500,000,000	web	hacked
Friend Finder Networks	2016	412,214,295	web	poor security / hacked
Massive American business hack	2012	160,000,000	financial	hacked
Adobe Systems	2013	152,000,000	tech	hacked
Under Armour	2018	150,000,000	Consumer Goods	hacked
eBay	2014	145,000,000	web	hacked
Equifax	2017	143,000,000	financial, credit reporting	poor security
Heartland	2009	130,000,000	financial	hacked
Rambler.ru	2012	98,167,935	web	hacked
TK / TJ Maxx	2007	94,000,000	retail	hacked
MyHeritage	2018	92,283,889	genealogy	unknown
AOL	2004	92,000,000	web	inside job, hacked
Anthem Inc.	2015	80,000,000	healthcare	hacked
Sony PlayStation Network	2011	77,000,000	gaming	hacked
JP Morgan Chase	2014	76,000,000	financial	hacked
National Archives and Records Administration	2009	76,000,000	military	lost / stolen media
Target Corporation	2014	70,000,000	retail	hacked
Tumblr	2013	65,469,298	web	hacked
Uber	2017	57,000,000	transport	hacked
Home Depot	2014	56,000,000	retail	hacked
Philippines Commission on Elections	2016	55,000,000	government	hacked
Facebook	2018	50,000,000	Social network	Poor security
Evernote	2013	50,000,000	web	hacked
Living Social	2013	50,000,000	web	hacked

Most common passwords (2017)

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123123
18. dragon
19. passw0rd
20. master
21. hello
22. freedom
23. whatever
24. qazwsx
25. trustno1

sources: https://vigilante.pw/, SplashDat

Multi-Factor Authentication (MFA)

What is it?

- You might also hear of 2FA (Two-Factor Authentication) which is a subset of MFA
- MFA is an authentication method that uses multiple independent credentials
  - What the user *knows*
  - What the user *has*
  - What the user *is*
- Adds another layer of security beyond username and password, which can be easily cracked, guessed, or hacked
- MFA has been around for many years, but is now starting to be common in the private sector

- What the user *knows:*
  - Password
  - PIN code
  - Security questions
- What the user *has:*
  - Security token
  - One-Time password (OTP)
  - ATM card
  - iOS/ Android app
- What the user *is:*
  - Fingerprint
  - Retina scan

BOSTON UNIVERSITY

Multi-Factor Authentication (MFA)

Why should I use it?

- The standard username and password authentication method necessarily requires a database of stored passwords. If this is captured, it is only a matter of time before the database will fall.
- As computers get more and more powerful, cracking passwords gets easier and easier
- MFA creates redundancy. If your password is compromised due to poor strength or a hack, there is still a fallback
- It is very easy to set up
- Hackers go after the easy targets. Don’t be one!

How do we use it at BU?

- We use an MFA solution called DUO at BU
- DUO protects our sensitive systems
  - BUWorks
  - Our Mainframe
  - Other sensitive data systems that contain PII
- DUO is easy to use:
  - Can ‘push’ notifications to DUO app (preferred)
  - Can receive an SMS one-time passcode
  - Can receive call to mobile or office phone

BOSTON UNIVERSITY