



12 Ways Multi-Factor Authentication can be Hacked and How to Best Defend Against It

Wednesday, June 22, 2022

Presented by:

KnowBe4
Human error. Conquered.








INTERWARE SYSTEMS



Presented by:
Marcus Ge, Head of GRC
Interware Systems

//////
ABOUT US
39th Year in Business

-  Cybersecurity
-  Digital Transformation
-  Cloud

- Healthcare
- Retail Chains
- Education
- Public Sector
- Financial Institutions
- Law Firms





INTERWARE SECaaS

WITH A HOLISTIC APPROACH

MDR Service



- ▶ 24/7/365 SOC
- ▶ Following NIST SP800-61
- ▶ Vendor certified security analysts
- ▶ Endpoint monitoring, incident detection, response, remediation and containment

GRC CONSULTING SERVICES



- ▶ Determine IS strategy
- ▶ Control objective and gap analysis
- ▶ Risk analysis
- ▶ Security policy build and review
- ▶ Cybersecurity awareness program

THREAT LANDSCAPE



61% of all breaches involve credentials, whether they be stolen via social engineering or hacked using brute force.



60% of mid-sized businesses that have asked their employees to work remotely experienced a cyberattack.



56% of those experienced credential theft.



48% experienced social engineering, such as phishing.



99% of IDSA's respondents who'd suffered an identity-related breach believe that these types of attack are preventable.



CASE: SONY PICTURES - ATTACKED BY G.O.P.

- Guardians of Peace - allegedly a hacker group from North Korea



QUICK OVERVIEW

NOV. 24

Wiper malware infects Sony Pictures' systems

DEC. 16

G.O.P. publishes a "terror" threat against movie theaters

DEC. 17

Sony Pictures cancels the Dec. 25 release of "The Interview"

DEC. 19

The FBI attributes the malware attack to North Korea

LESSONS LEARNED:

- Everyone is a target
- Put qualified and proactive people in information security roles
- Don't make a hacker's job too easy
- Security starts from management



BUILDING GOOD POLICY

- It's difficult to build compliance to follow regulation.
- Security compliance is a requirement for all companies, users will always try to find a shortcut or to bypass it.
- It's more and more prominent in this landscape to have good credential practices.





A MOVING TARGET

- Technology moves forward
- Moore's Law - Passwords become more and more convoluted.
- In 2005, it took over 6 days to crack the password "secures1".
- 10 years later, it took 2 days.

Can anyone guess how long it would take today?





HOW CAN WE PROTECT OURSELVES?

- ▶ Adding letters to your numbers / vice-versa
 - 123456789 = cracked 431 times in the blink of an eye
 - A23456789 = will be cracked when Oscar award winner Leonardo DiCaprio is 84 years old



HOW CAN WE PROTECT OURSELVES?

- ▶ Combining ASCII
 - Password = cracked just under the time it would take for lightning to strike 2 times
 - P@ssw0rD = will be cracked in the same amount of time it took to carve Mount Rushmore
- ▶ Even this we do not recommend to our clients who truly want to protect themselves from risk
- ▶ Cyber insurance is a must have





HOW CAN WE PROTECT OURSELVES?

- ▶ Implement Multi-Factor Authentication
- ▶ Everyone knows
- ▶ MFA is an added step, but a necessary one



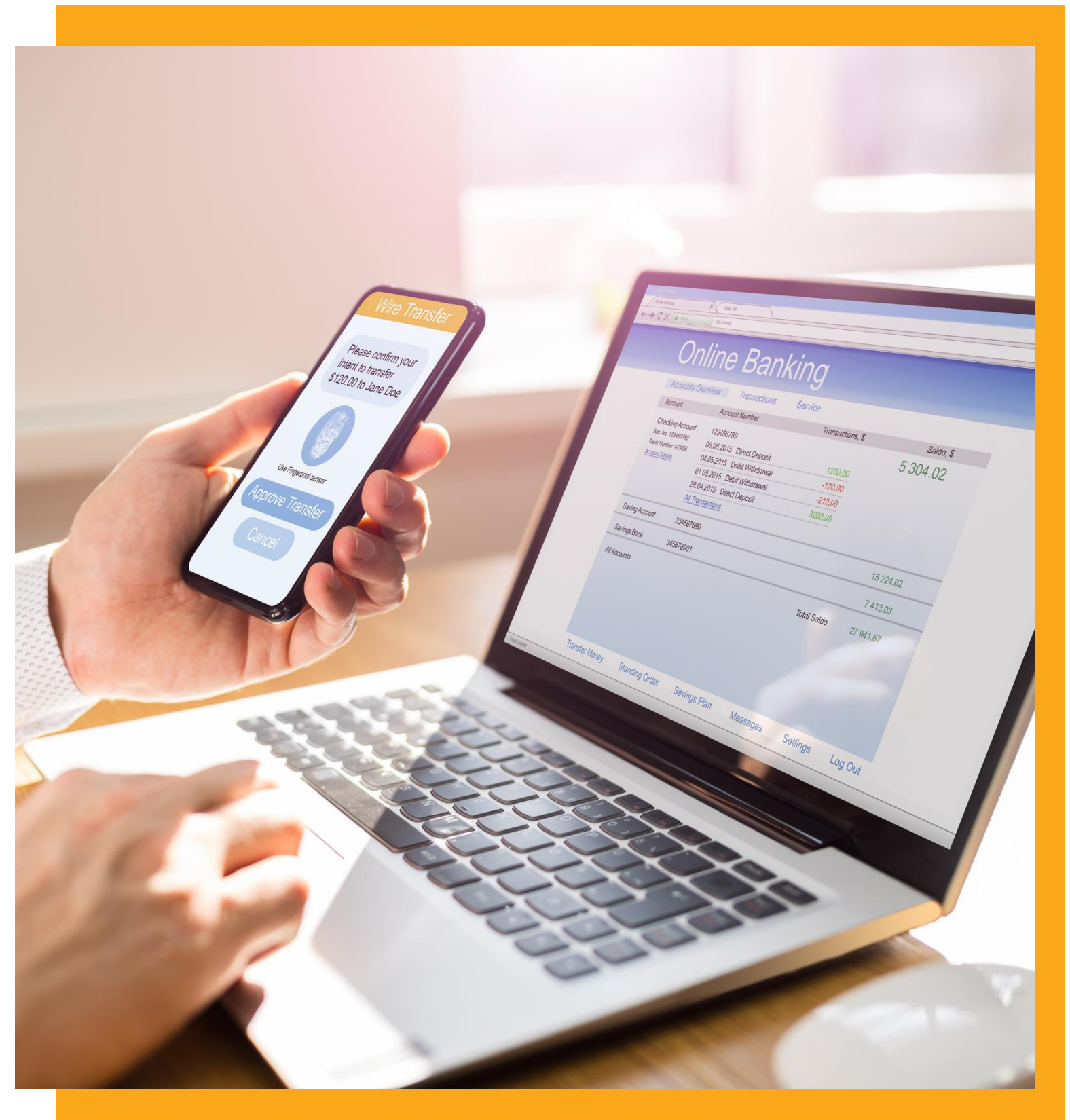


DIVING INTO MFA

From technical standpoint, let's analyze MFA.
There are ways to defeat it.

You will learn:

- Ways to compromise
- Ways to circumvent
- Ways to implement it properly!





INTRODUCING



PRESENTED BY:
ROGER GRIMES
DATA-DRIVEN EVANGELIST