What Do Joe Biden & Kim Kardashian Have In Common?

Michael Wylie, MBA, CISSP
About Dr. TPN:

Michael Wylie, MBA, CISSP
Director, Cybersecurity Services
RICHEY MAY TECHNOLOGY SOLUTIONS

Additional

- GPEN
- GMON
- CEH
- CEI
- TPN
- GCFE

Certifications

- CCNA R&S
- CCNA CyberOps
- Project+
- Pentest+
- Security+
About Richey May Technology Solutions

Cybersecurity

Content Security

Governance, Risk, Compliance & Privacy

Technology Management

Business Intelligence

Cloud Services

Penetration Testing

Cloud Workflow Integration

Secure Network Architecture

TPN Assessments & Readiness

Vulnerability Scanning

Forensics & Incident Response

Content Protection

Cloud Services

Technology Management

Business Intelligence

Governance, Risk, Compliance & Privacy

Cybersecurity

Content Security
• We’ve all completed security awareness training
• We’ve all seen a phishing email or two
• MPA/TPN requires awareness training
• Can clicking a link or sharing a password really that big of a deal?

What if I told you a story about how a group of people tried to rob a bank for one billion dollars and it all started with a phishing email?

But first, ”What Do Joe Biden & Kim Kardashian Have In Common?”
What Do Joe Biden & Kim Kardashian Have In Common?

Joe Biden
@JoeBiden - 32s
I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkgjhx0wlh

Enjoy!

Kim Kardashian West
@KimKardashian

Feeling nice! All BTC sent to my will be sent back doubled, enjoy.

bc1qwr30ddc04zqp878c0evdrqfx564mmf0dy2w39l

10:05 PM · 15/07/2020 · Twitter Web App
"We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools..."
My Work Life Before the Pandemic / My Work Life During the Pandemic

March 2020

October 2020

* No babies were harmed during the photo shoot.
According to an affidavit:

“[a 17-year-old] used social engineering to convince a Twitter employee that he was a co-worker in the IT department and had the employee[s] provide credentials to access the customer service portal.”

Incidents are more impactful because:

- Disperse workforce
- Flex hours
- Workplace distractions (e.g. virtual schooling)
- Attackers are preying on the opportunities
Bangladesh Bank Heist

Bangladesh Bank heist
In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines.

THE MONEY TRAIL

Transaction date

FEB. 4-5, 2016

$951 million
35 orders
Via New York Fed
Via SWIFT global bank messaging system

FEB. 5-13

$101 million
5 orders
Via RCBC

$81 million
Four U.S. dollar accounts
Via Philrem

$31 million
RECIPIENT
Weikang Xu

$29 million
RECIPIENT
Solaire*

$20 million
RECIPIENT
Shalika Foundation

$21 million
RECIPIENT
Eastern Hawaii Leisure Co.

* A casino resort owned and operated by Bloomberg Resorts

Sources: Philippines Court of Appeals documents; Reuters
W. Foo, 31/03/2016
Hi my name is Tamera
attach is my resume
Your early reply will be appreciated

Sincerely

Tamera
Security Testing is NOT:

- Just someone trying to hack you
- An inexperienced person running scans
- Evidence that you’re secure
- A $750 commodity
- Something to take lightly

Security Testing is:

- A collaborative experience to fortify your defenses
- A simulated attack performed by a highly skilled ethical hacker
- A point-in-time test of certain security controls
- An opportunity to identify false assumptions and build better controls
- An opportunity to find vulnerabilities and fix them before criminals exploit them
“Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability (source: NIST SP800-115).

Note: A vulnerability scan alone does not always suffice as a penetration test.”

Email me for a real penetration test report: Michael@RicheyMay.com
Security Professionals at Work
Richey May Cuts Down on Video Game Time
This is Not How You Simplify Security
You’re Only As Strong As Your Weakest Link