Navigating the Virtual Highway:

Cybersecurity Tips and Best Practices

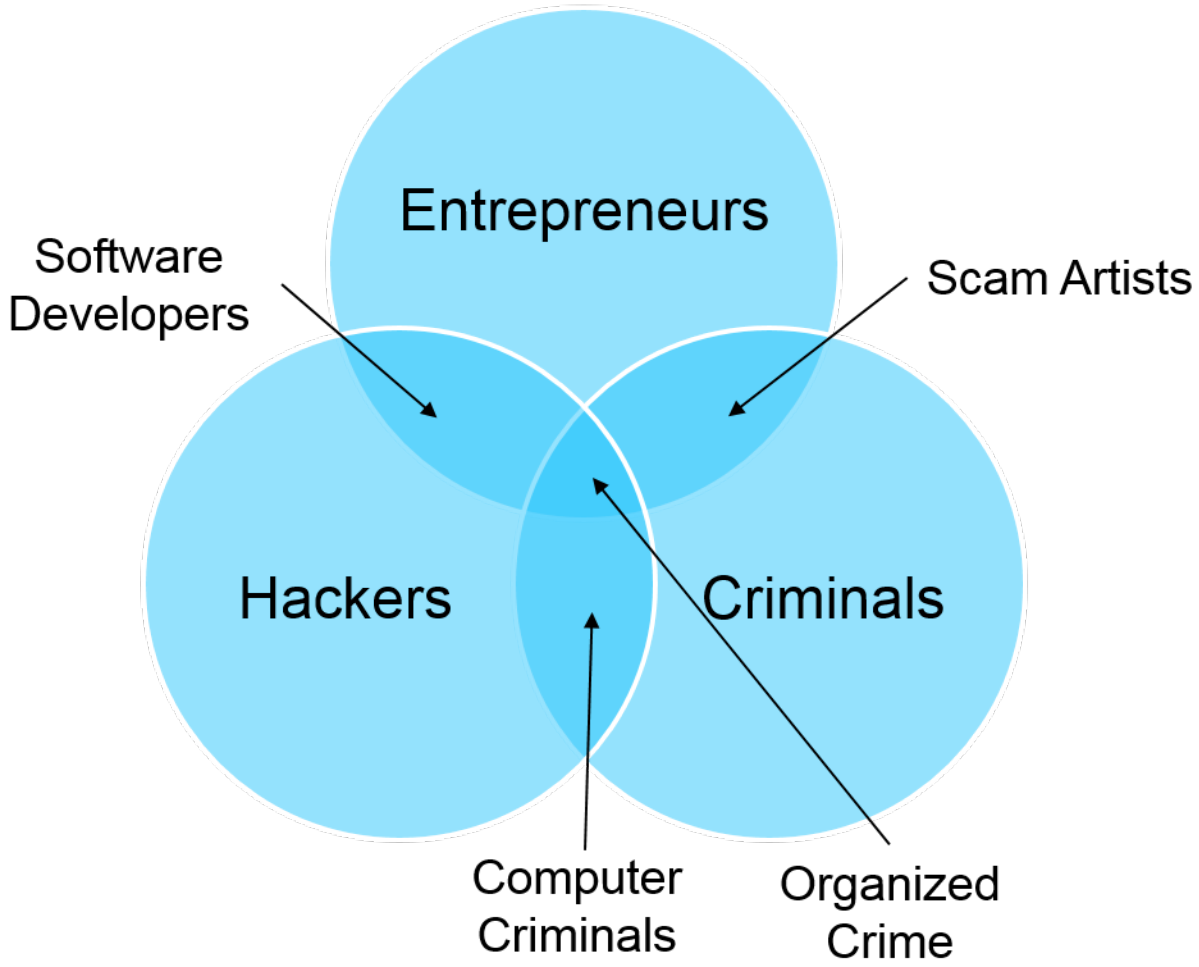
Presented by: Scott Thompson, MERS IT Director

Computing and Cybersecurity 70 Years Ago

The “Good Ol’ Days” of Cybersecurity

70 YEARS

The New Normal – Today's Cybercriminal



The New Normal – Today's Cybercriminal

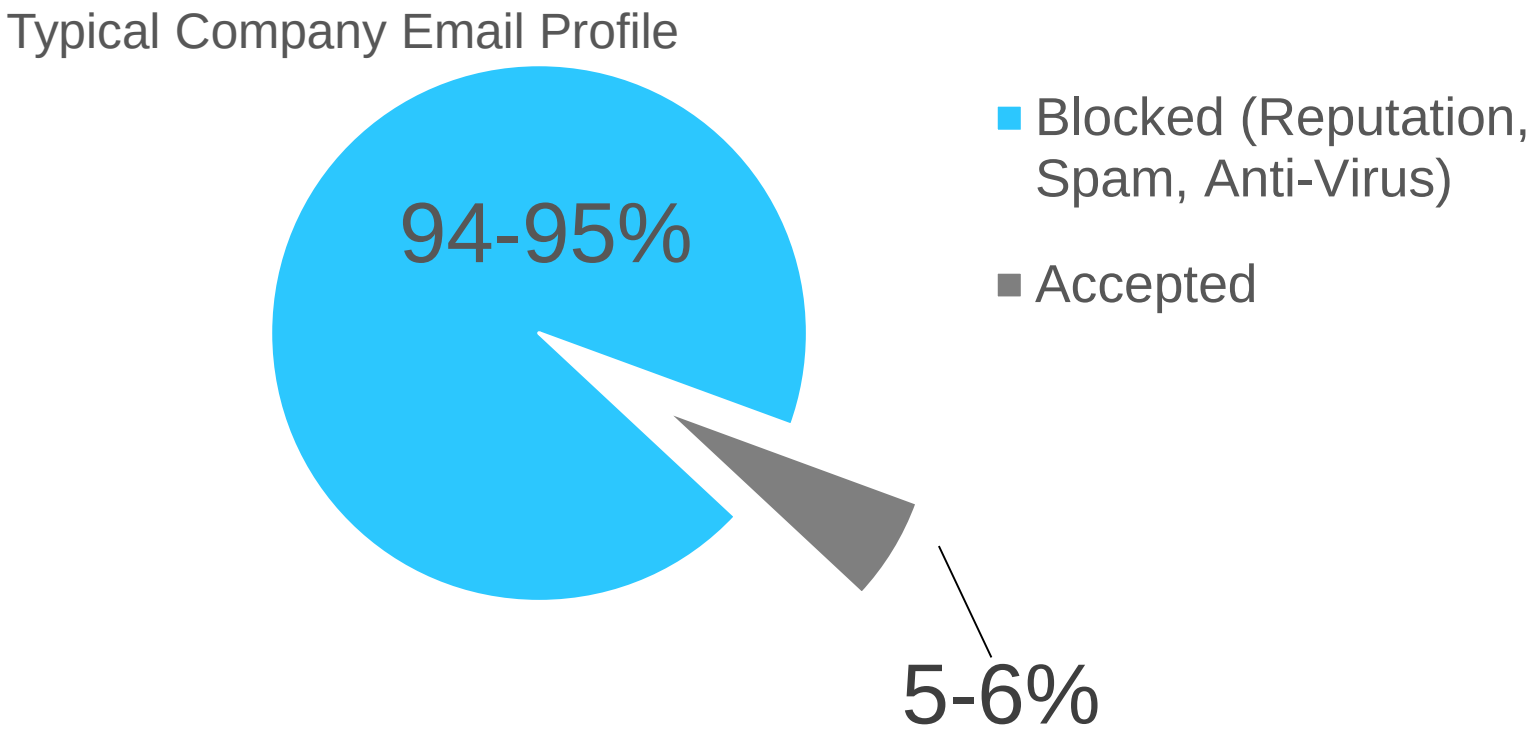
70 YEARS

Typical Daily Sources of Cyber Attacks

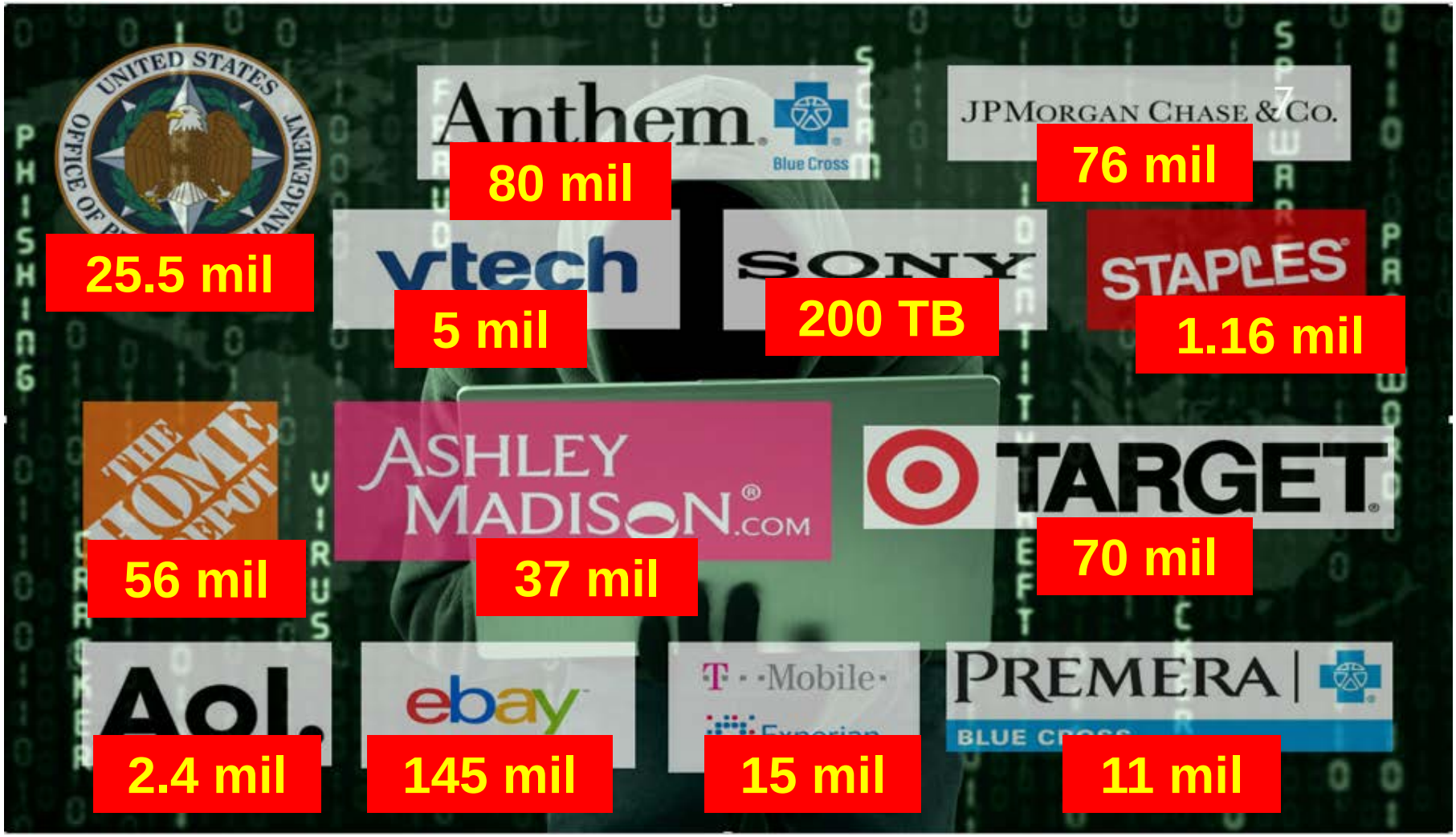
70 YEARS

Company Email Under Siege

In a typical company, what percentage of email is safe?



Cost of a Data Breach



Data Breach Impacts

- Data breaches can have a devastating impact on an organization
- The average cost of a breach ranges $154 to $1,000 per record
- A breach of just 1,000 records could cost $1M, not including any ransom that may be paid

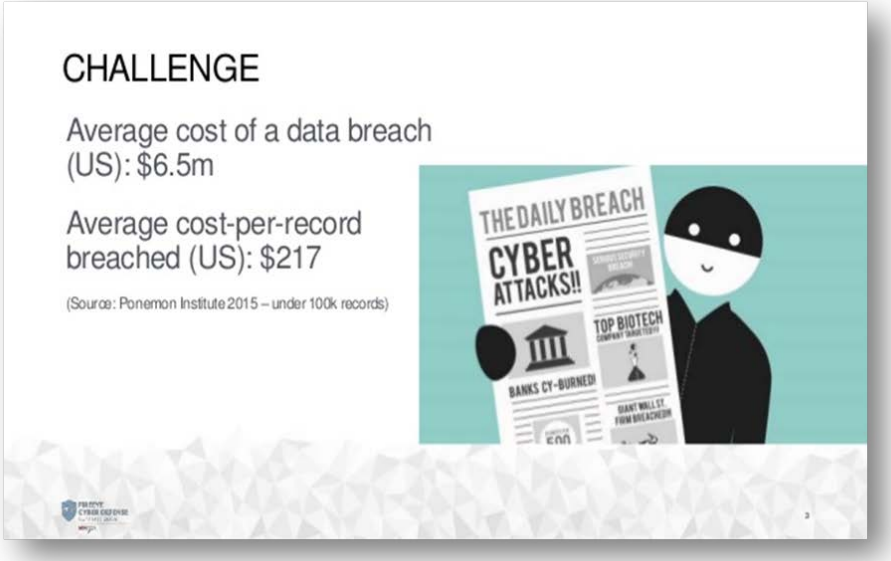
Data Breach Damages Include

Direct Damages

- Professional services (investigation and remediation, etc.)
- Lost business opportunities (disclosure, public reputation, etc.)
- Down-time

Indirect Damages

- Staffing increases and changes
- Increased employee training
- System repair and improvements
- Increased insurance costs

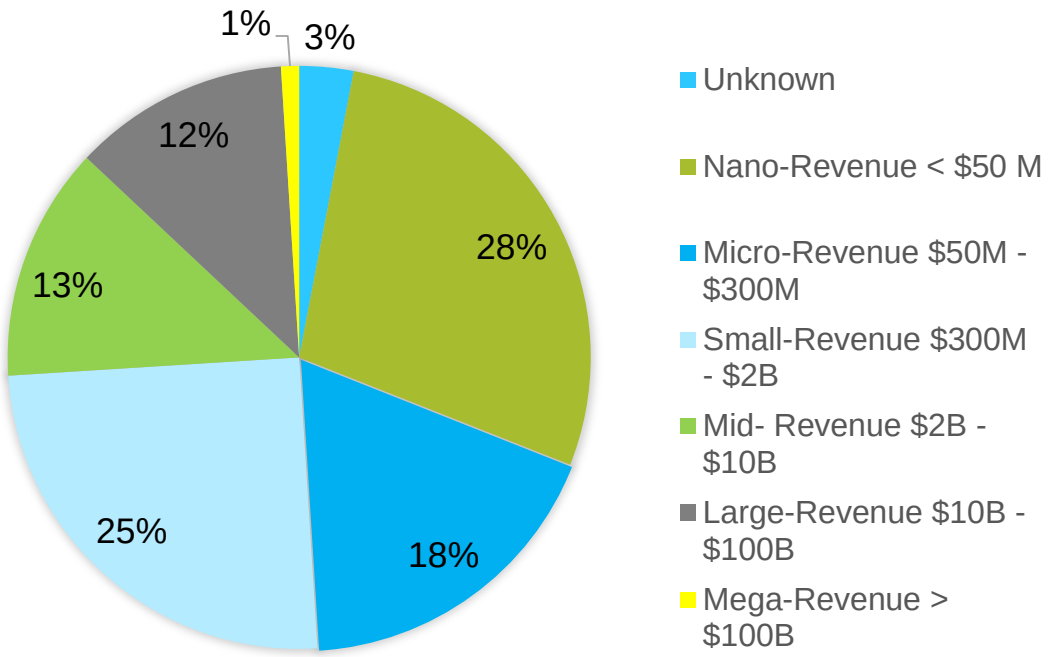


Types of Cybersecurity Incidents Today

- Locky Ransomware hack currently infecting 90K machines per day
- Recent federal bank system hack resulted in $80M stolen in 3 bank transfer requests
- Social engineering email hack for boss on vacation requesting bank EFT
- W-2 Social Engineering Scams
- 2016 IRS Tax Submittal Scams

No Safe Haven…

Percentage of Claims by Revenue Size



Compiled from:
- NetDiligence/McGladrey 2015 Annual Cyber Claims Study

70 YEARS

Social Engineering and Phishing Scams

- Trickery or deception for the purpose of information gathering, fraud, or computer system access
- In most cases the attacker never comes face-to-face with the victim

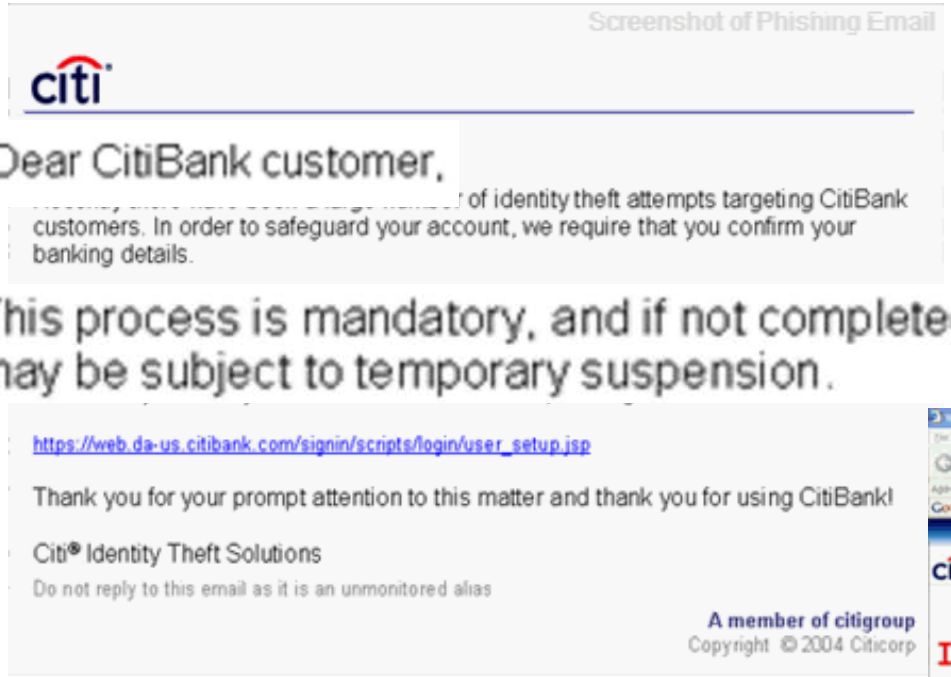
Common Social Engineering Methods

There are methods and attack techniques that are used by prospective criminals:

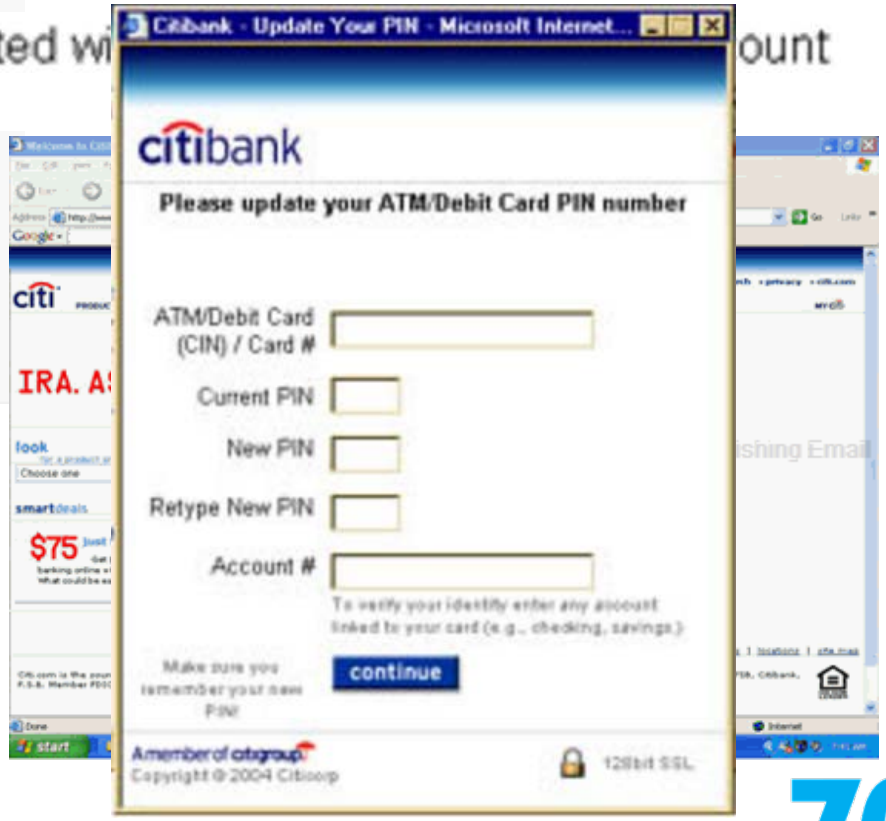
- Public Wi-Fi/Hotel Wi-Fi
- Tailgating (i.e. access a secure building or secure area)
- Baiting (i.e. purposely leaving media such as CD-ROM or a flash drive to be picked up and plugged in)
- Phishing/Trick-to-click

70 YEARS

Phishing Lures



These email and website examples are relatively easy to distinguish

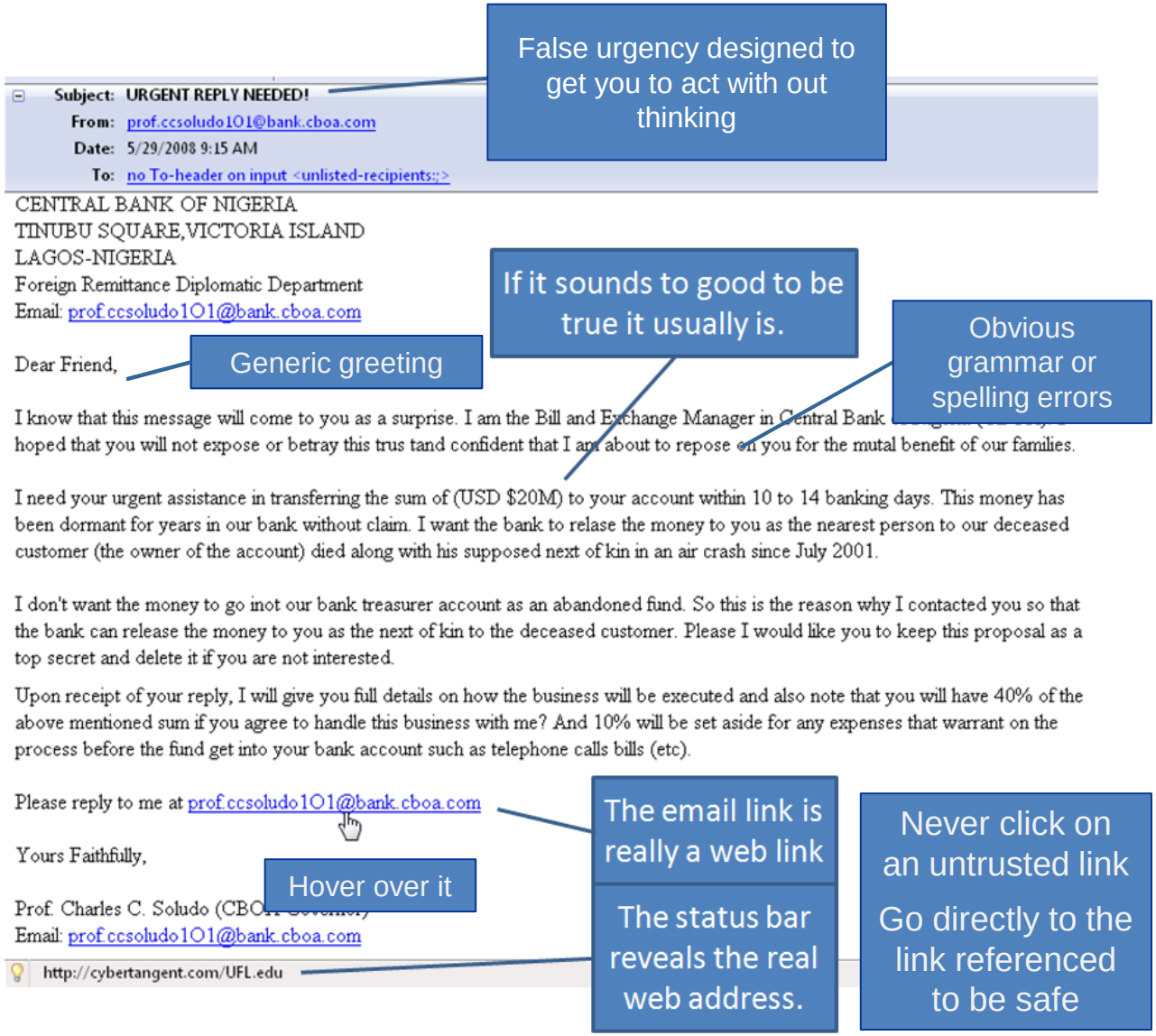


The more applicable or urgent the scenario, the greater risk of falling prey to phishing

- FBI, legal threats for non-reply
- UPS message at Christmas
- Resend W-2 forms at tax time, etc.

70 YEARS

Phishing Lures Targeting Retirees



Statistics

- Sweepstakes and lottery scams alone trick Americans out of **billions** of dollars every year
- An estimated 10%–15% of the U.S. population fall victim each year
- Average age is 55–65 years old
- Scams under-reported
  - Most too ashamed to report being victimized
  - More than 90% of lottery scams not reported

(Source: AARP)

70 YEARS

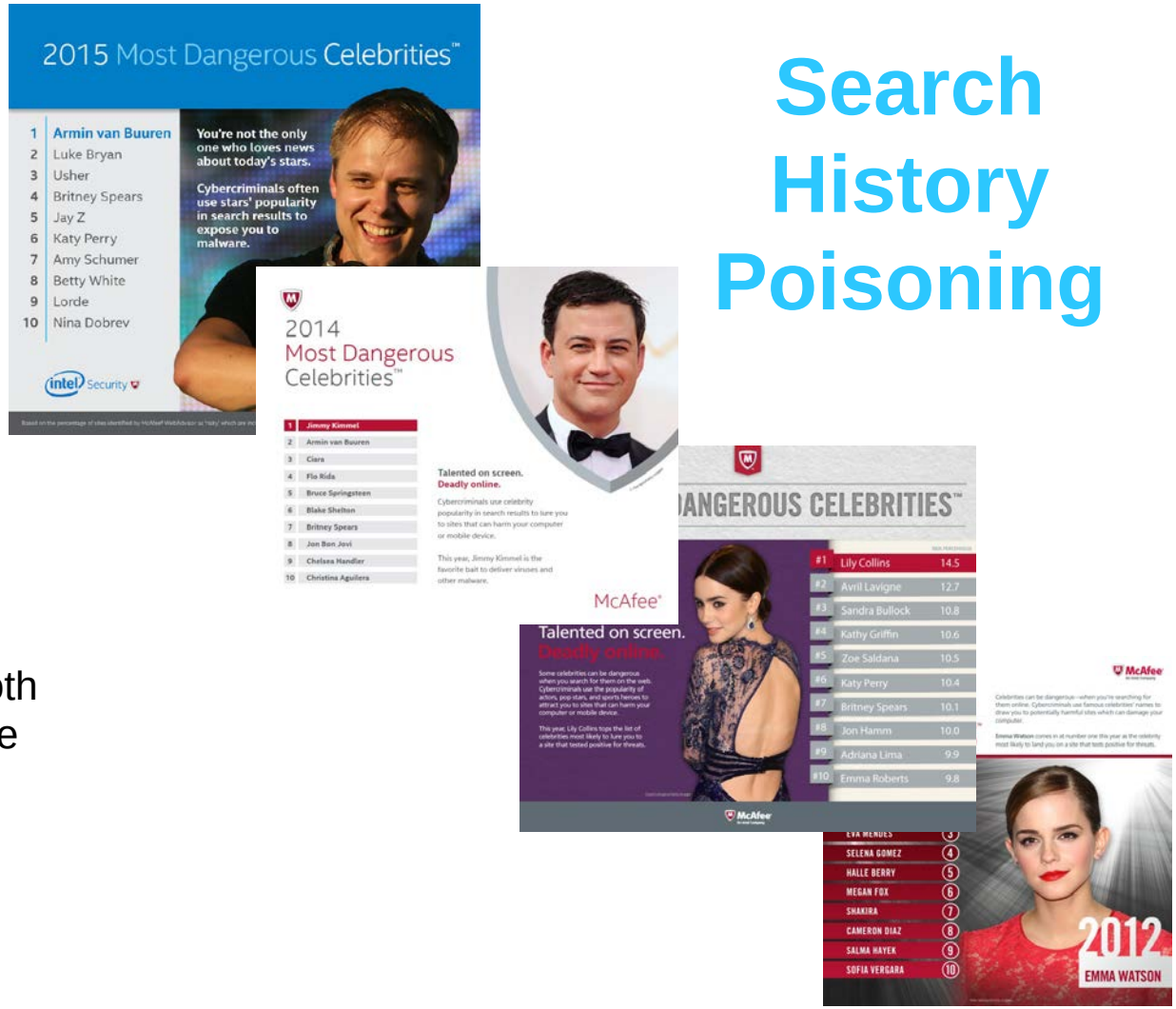
When Communicating with MERS

Tips to securely communicate and transact business with MERS:

- Don’t reply directly to e-newsletters, event notifications or any other type of mass email. Contact the MERS Service Center if you have any questions about the information you receive
- Use your secure myMERS account to transact MERS business such as changing your investment allocations and updating your contact information
- Use the tips we just learned to ensure that all emails that appear to be coming from a MERS address (ex:jdoe@**mersofmich.com**) aren’t phishing scams
- Report any suspicious emails or other forms of communication that appear to be coming from MERS to the Service Center

The Most Dangerous Person on the Internet (McAfee)

- 2015 - Armin Van Buuren
- 2014 - Jimmy Kimmel
- 2013 - Lily Collins
- 2012 - Emma Watson
- 2011 - Heidi Klum
- 2010 - Cameron Diaz
- 2009 - Jessica Biel

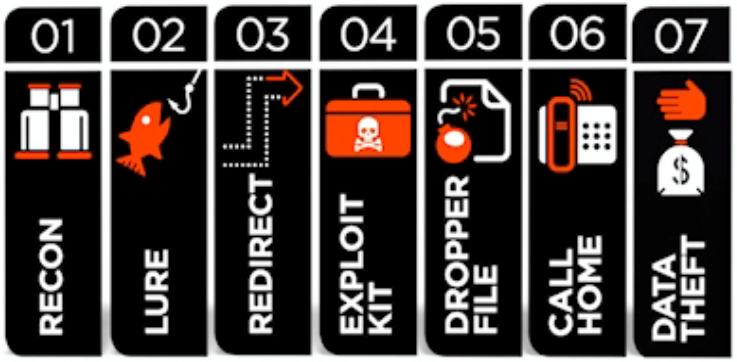


Search History Poisoning

Jessica Biel and Megan Fox both dropped off the 2013 list despite previously placing in the No. 2 and No. 6 spots because they became too popular

70 YEARS

Sophisticated Phishing Chain



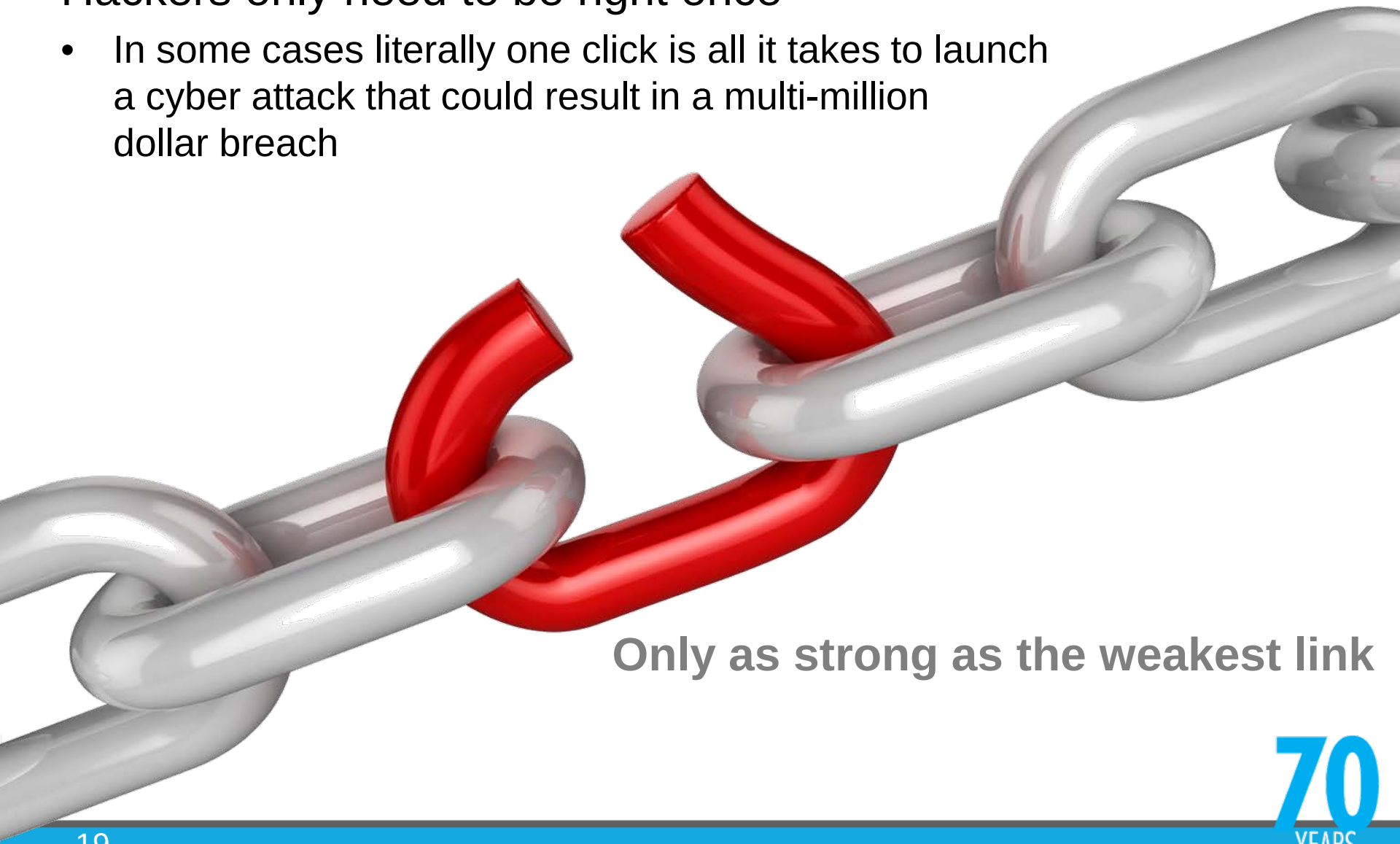
Professional, methodical approach to steal data:

- Initial reconnaissance
- Crafting a phishing lure (trick-to-click)
- Redirecting victim to a compromised server
- Use an exploit kit to scan for vulnerabilities
- Drop malware onto the victim's device
- Call home to the command and control server
- Exfiltrate (or encrypt) data and control the workstation

Cybersecurity Realities

Hackers only need to be right once

- In some cases literally one click is all it takes to launch a cyber attack that could result in a multi-million dollar breach



Only as strong as the weakest link

Cybersecurity Realities, Cont.

- Survival of the fittest
  - Cybersecurity's premise is to make it so difficult for hackers that they attack other targets, but not make it more difficult for business users or customers
- Social engineering is on the rise
  - Hackers want a Trojan Horse solution
  - If the fortress is impenetrable, trick someone into opening a door

70 YEARS

Cybersecurity Realities, Cont.

Comprehensive cybersecurity solutions must involve a combination of investments

process

Cybersecurity is not a turn-key solution, it's a lifecycle

people

Maintain cybersecurity training and expertise (core of cybersecurity)

technology

Cybersecurity tools, applications, and infrastructure

Cybersecurity is a ongoing commitment

70 YEARS

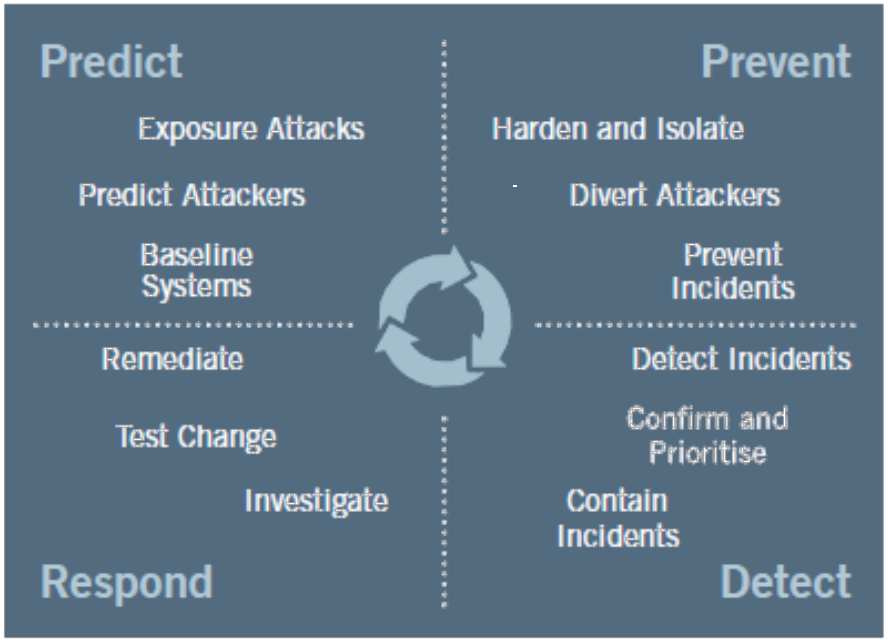
MERS Cybersecurity Risk Mitigations

- Encryption of sensitive data in transit
- Routine security awareness training for all employees
- Company wide internal phishing testing
- Consistent vulnerability testing and remediation
- InfraGard membership
- Cybersecurity maturity assessment

Effective Cyber Security Controls

Incident Response Planning

- Threat level definitions
- Escalation/de-escalation criteria and procedures
- Technology and business roles, responsibilities and authority
- Formal cyber-incident communication triggers and procedures



Source: Gartner, 2015

70 YEARS

Access Controls and Password Security

- Rather than thinking of your passwords as an annoyance, think of your passwords like your keys, wallet or purse
- Like a wallet or keys, a password is used to prove identity or gain access to a resource and is just as risky to lose

A poor password can directly impact your wallet!

“The Trifecta” – Bad Password Mistakes

- Reuse of passwords
  - Using the same password for multiple systems
- Bad password storage and management
  - Sticky notes, taped under keyboard, an unsecured spreadsheet, not changing passwords within reasonable time frames, etc.
- Poor password selection
  - Selecting easily guessed passwords

What Makes a Good Password?

- Examples of good password practices
  - Use a familiar phrase with phonic/symbol replacements
    IH8P@$$w0rd$
  - The name of the site with phonic/symbol replacements
    MER$0fM1ch
  - Good for managing different passwords for most sites
- MERS portal password change policy update
  - Banking industry password problems driving changes

Importance of Complex Passwords

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
16	1 year	512m years	1bn years	6tn years	193tn years

How long will it take to hack YOUR password?

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Internet and Social Media Cybersecurity

There are 7.2 billion people in the world

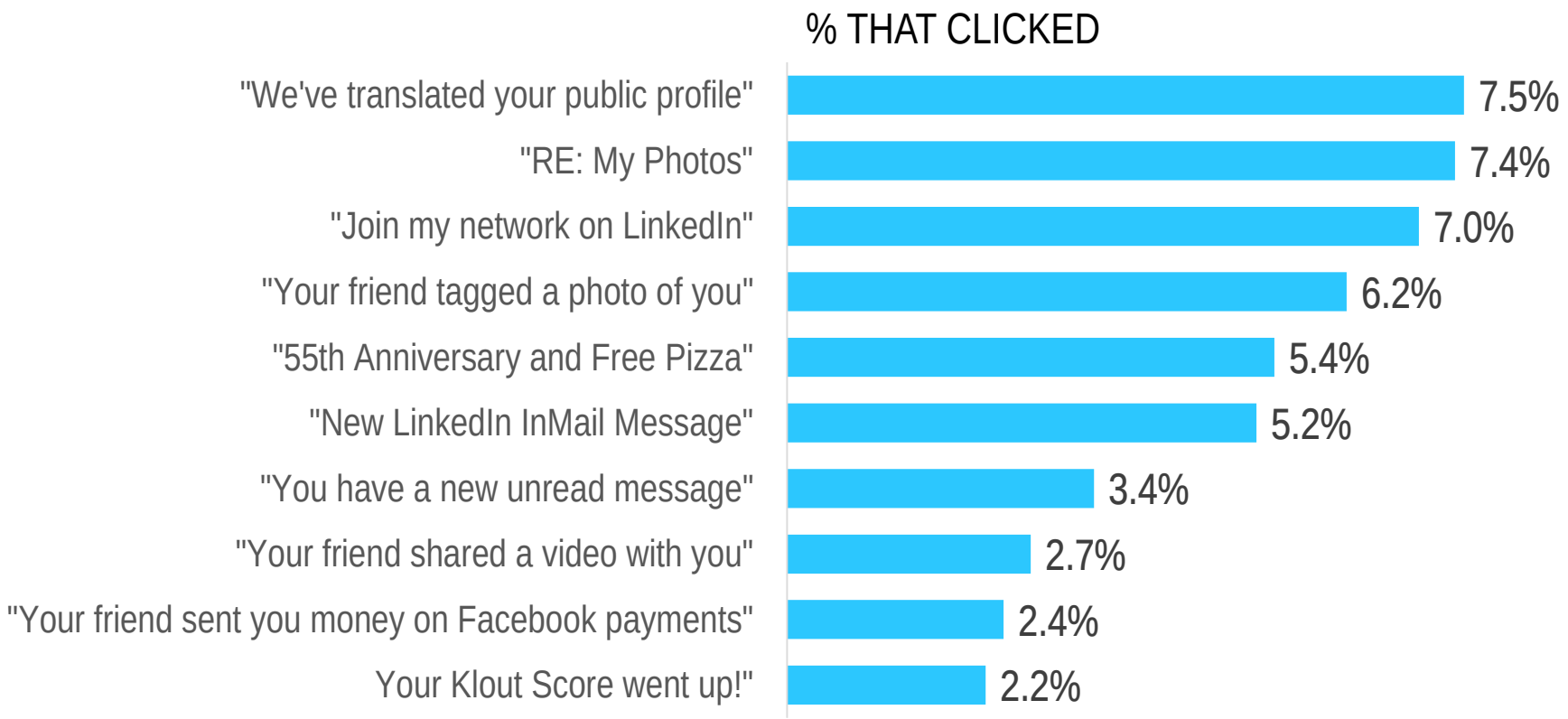
3 billion of them are internet users

2 billion of those are active on social media

- Facebook alone has 1.3 billion users
- Google+ has 540 million active users
- Twitter has 294 million active users
- LinkedIn has 187 million active users

Common Social Media Scams

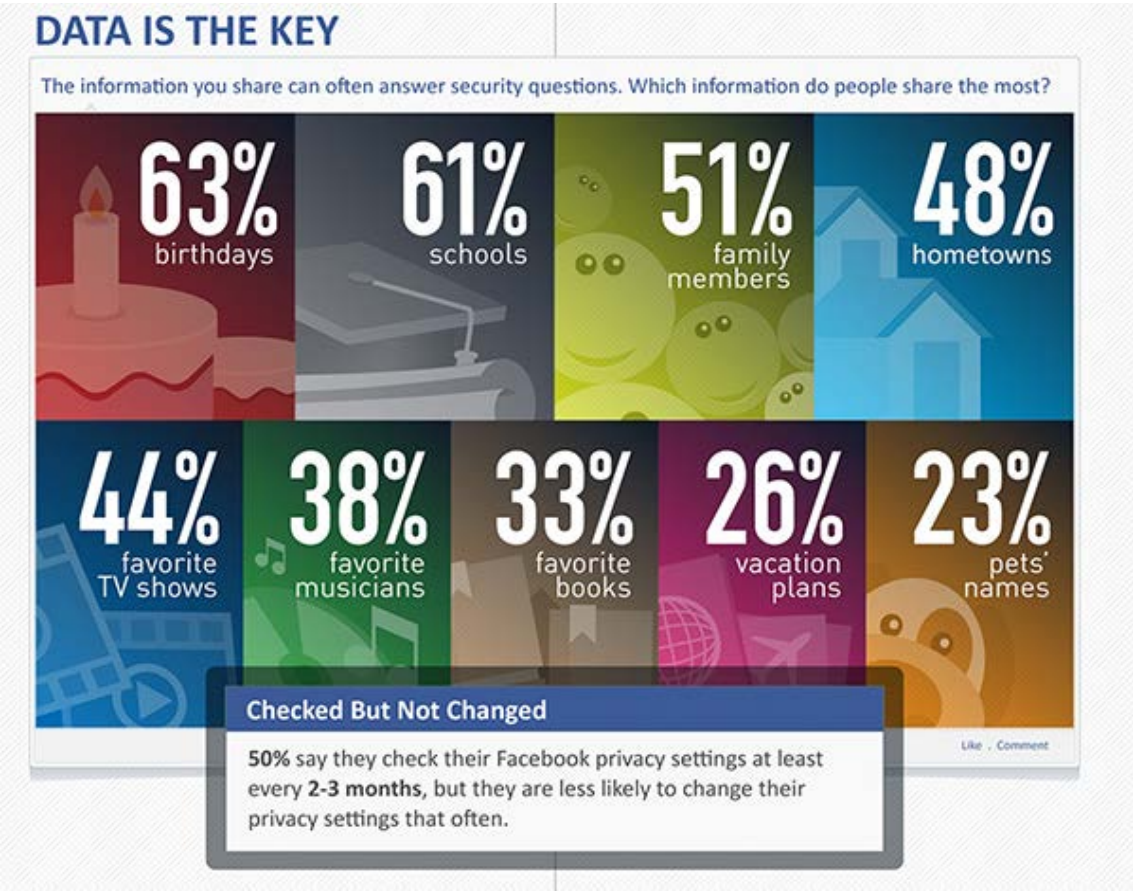
This year's most clicked social media scam lines



Source: KnowBe4

Social Media Dangers

- "TMI" – People are oversharing personal and company information, which can be dangerous
- Targeted phishing attacks ("spear phishing") can be built against you or your family, employees, colleagues or friends based on this type of information



70 YEARS

Social Media Do's and Don'ts

DON'T

- Post Personally Identifiable Information (PII), Personal Health Information (PHI), or other sensitive data that can be used for identity theft
- Post information about your organization structure and relationships if not needed
- Post schedule, vacation or location information unless afterward
- Use the same password for multiple sites

DO

- Use social media sites for intended purpose
- Supply the minimum information necessary to complete your intended purpose
- Understand the personal and professional risks being taken with social media
- Take any cybersecurity training available prior to using social media
- Update privacy settings regularly

Cybersecurity Readiness

- Cybersecurity Readiness is like Retirement Readiness
  - It's about planning for the future (breach)
    - For most companies it is not about "If", it is about "When"
  - Assumptions are made for retirement (cybersecurity)
  - Upfront investments are required to have retirement (cybersecurity)
- Cybersecurity is a never-ending journey
  - Risks evolve
  - Cybersecurity is like chess
  - Reflection is important

70 YEARS

Summary/Conclusion

- Cybersecurity awareness / phishing recognition
  - Build employee, customer and vendor cybersecurity expertise
  - Constantly work to mitigate your weakest links
- Cyber events, incidents and breaches
  - Attacks will happen, be prepared
  - Cybersecurity Readiness is as important as Retirement Readiness
- Cybersecurity trends
  - Social engineering and ransomware are growing at an alarming rate
  - Cybersecurity is a never-ending commitment

MERS is committed to keeping your data safe!

70 YEARS

Contacting MERS

MERS of Michigan
1134 Municipal Way
Lansing, MI 48917

Phone: 800.767.6377
www.mersofmich.com

LET'S GET SOCIAL!