

# Navigating the Virtual Highway:

*Cybersecurity Tips and Best Practices*

*Presented by: Scott Thompson, MERS IT Director*

PLANNING  
RETIREMENT  
TOGETHER FOR

70  
YEARS



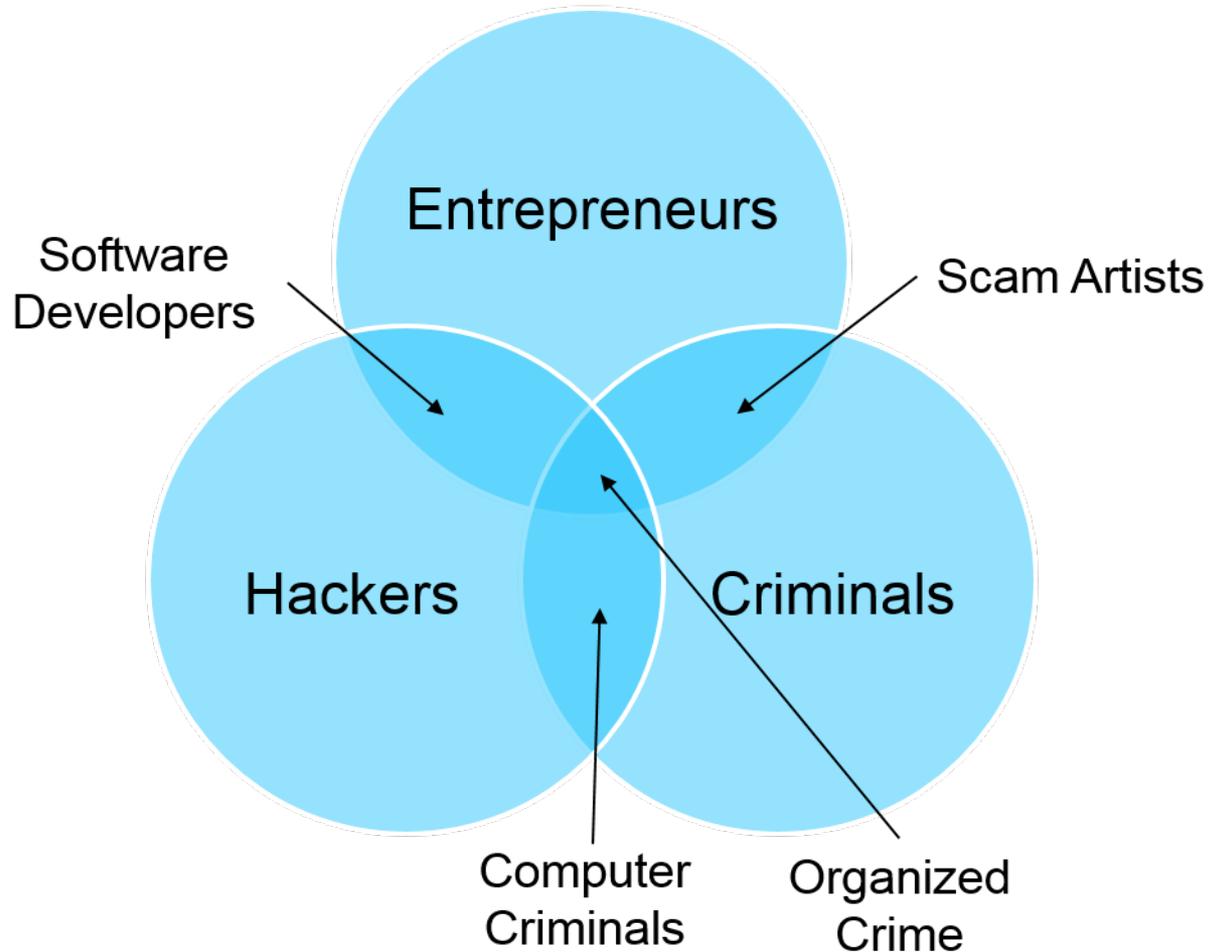
# Computing and Cybersecurity 70 Years Ago



# The "Good Ol' Days" of Cybersecurity



# The New Normal – Today's Cybercriminal



# The New Normal – Today's Cybercriminal



Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

**EVGENIY MIKHAILOVICH**

urs



# FBI

**\$100,000  
Rewards**

Aliases:  
Yevgeniy Bogachev, Evge

# Most Wanted Hackers



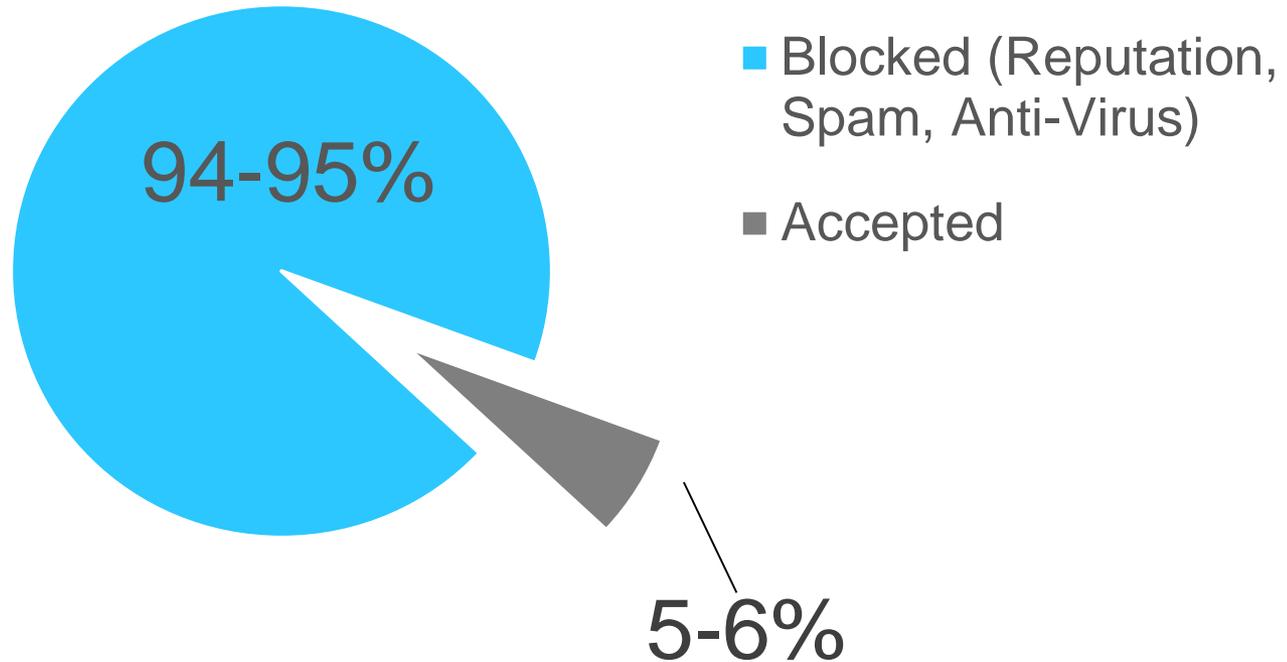
# Typical Daily Sources of Cyber Attacks



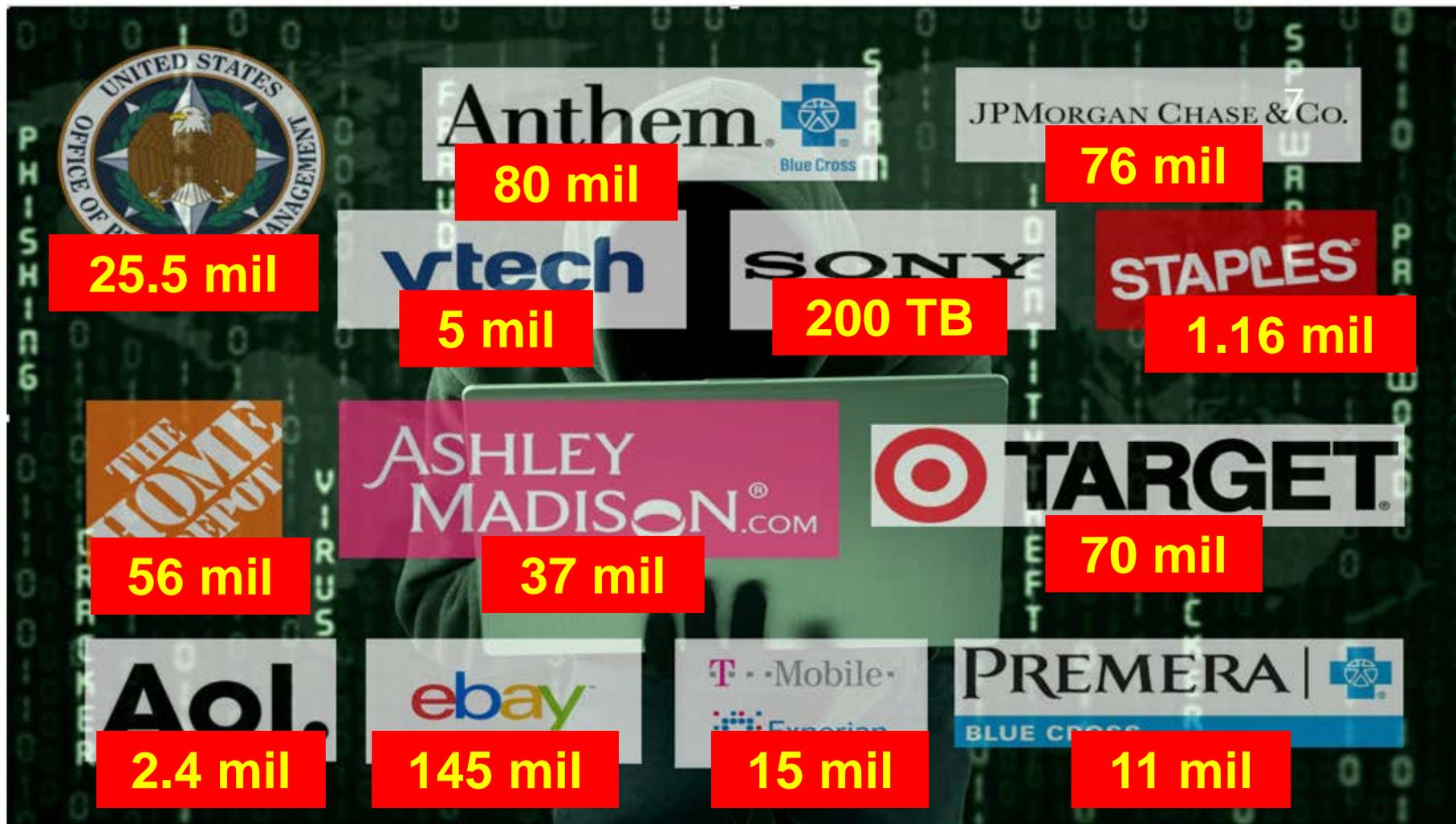
# Company Email Under Siege

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

Typical Company Email Profile



# 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

### CHALLENGE

Average cost of a data breach (US): \$6.5m

Average cost-per-record breached (US): \$217

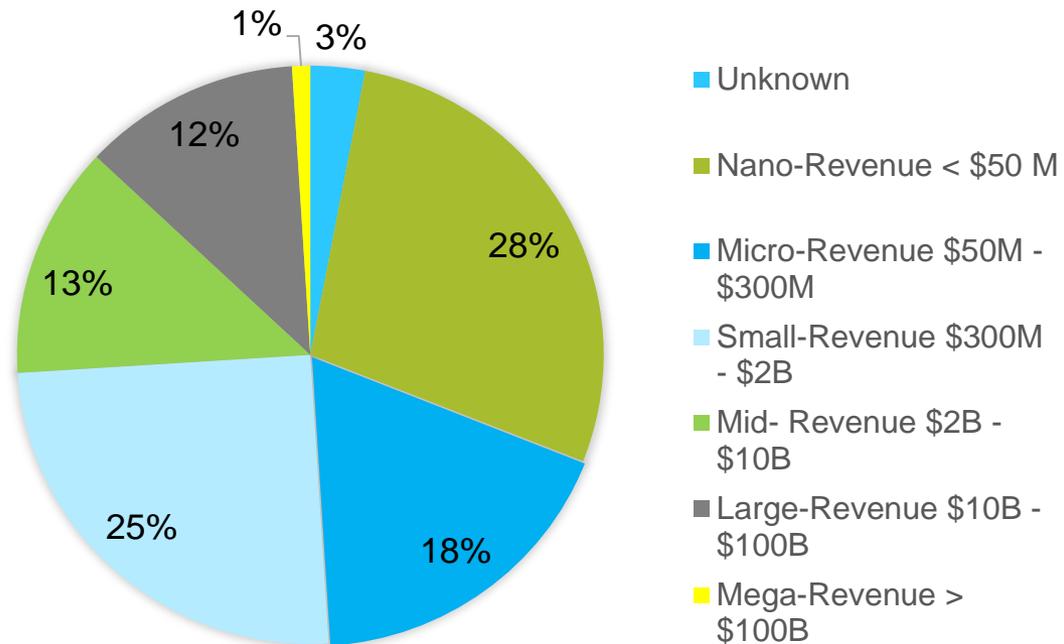
(Source: Ponemon Institute 2015 – under 100k records)



# 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

# 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



# Phishing Lures

Screenshot of Phishing Email



Dear CitiBank customer,

of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed with your account may be subject to temporary suspension.

[https://web.da-us.citibank.com/signin/scripts/login/user\\_setup.jsp](https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp)

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup  
Copyright © 2004 Citicorp

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.

These email and website examples are relatively easy to distinguish



# Phishing Lures Targeting Retirees

**Subject:** URGENT REPLY NEEDED!  
**From:** [prof.ccsoludo101@bank.cboa.com](mailto:prof.ccsoludo101@bank.cboa.com)  
**Date:** 5/29/2008 9:15 AM  
**To:** no To-header on input <unlisted-recipients:>

CENTRAL BANK OF NIGERIA  
TINUBU SQUARE, VICTORIA ISLAND  
LAGOS-NIGERIA  
Foreign Remittance Diplomatic Department  
Email: [prof.ccsoludo101@bank.cboa.com](mailto:prof.ccsoludo101@bank.cboa.com)

Dear Friend,

I know that this message will come to you as a surprise. I am the Bill and Exchange Manager in Central Bank. I hoped that you will not expose or betray this trust and confidant that I am about to repose on you for the mutual benefit of our families.

I need your urgent assistance in transferring the sum of (USD \$20M) to your account within 10 to 14 banking days. This money has been dormant for years in our bank without claim. I want the bank to relase the money to you as the nearest person to our deceased customer (the owner of the account) died along with his supposed next of kin in an air crash since July 2001.

I don't want the money to go inot our bank treasurer account as an abandoned fund. So this is the reason why I contacted you so that the bank can release the money to you as the next of kin to the deceased customer. Please I would like you to keep this proposal as a top secret and delete it if you are not interested.

Upon receipt of your reply, I will give you full details on how the business will be executed and also note that you will have 40% of the above mentioned sum if you agree to handle this business with me? And 10% will be set aside for any expenses that warrant on the process before the fund get into your bank account such as telephone calls bills (etc).

Please reply to me at [prof.ccsoludo101@bank.cboa.com](mailto:prof.ccsoludo101@bank.cboa.com)

Yours Faithfully,

Prof. Charles C. Soludo (CBOI Governor)  
Email: [prof.ccsoludo101@bank.cboa.com](mailto:prof.ccsoludo101@bank.cboa.com)

<http://cybertangent.com/UFL.edu>

**False urgency designed to get you to act with out thinking**

**Generic greeting**

**If it sounds to good to be true it usually is.**

**Obvious grammar or spelling errors**

**The email link is really a web link**

**Never click on an untrusted link**

**Go directly to the link referenced to be safe**

**Hover over it**

**The status bar reveals the real web address.**

## 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)

# 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

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

## Search History Poisoning

**2015 Most Dangerous Celebrities™**

1	Armin van Buuren
2	Luke Bryan
3	Usher
4	Britney Spears
5	Jay Z
6	Katy Perry
7	Amy Schumer
8	Betty White
9	Lorde
10	Nina Dobrev

You're not the only one who loves news about today's stars. Cybercriminals often use stars' popularity in search results to expose you to malware.

Based on the percentage of sites identified by McAfee's Malware as they search for the

**2014 Most Dangerous Celebrities™**

1	Jimmy Kimmel
2	Armin van Buuren
3	Ciara
4	Flo Rida
5	Bruce Springsteen
6	Blake Shelton
7	Britney Spears
8	Jon Bon Jovi
9	Chelsea Handler
10	Christina Aguilera

Talented on screen. Deadly online. Cybercriminals use celebrity popularity in search results to lure you to sites that can harm your computer or mobile device.

This year, Jimmy Kimmel is the favorite bait to deliver viruses and other malware.

**2013 Most Dangerous Celebrities™**

#1	Lily Collins	14.5
#2	Avril Lavigne	12.7
#3	Sandra Bullock	10.8
#4	Kathy Griffin	10.6
#5	Zoe Saldana	10.5
#6	Katy Perry	10.4
#7	Britney Spears	10.1
#8	Jon Hamm	10.0
#9	Adriana Lima	9.9
#10	Emma Roberts	9.8

Talented on screen. Deadly online. Some celebrities can be dangerous when you search for them on the web. Cybercriminals use the popularity of actors, pop stars, and sports heroes to attach you to sites that can harm your computer or mobile device.

This year, Lily Collins tops the list of celebrities most likely to lure you to a site that lures visitors for threats.

McAfee

CELEBRITIES CAN BE DANGEROUS - when you're searching for them online, Cybercriminals use famous celebrities' names to lure you to potentially harmful sites which can damage your computer.

Emma Watson comes in at number one this year as the celebrity most likely to lure you to a site that lures visitors for threats.

3	EVA MENDES
4	SELENA GOMEZ
5	HALLE BERRY
6	MEGAN FOX
7	SHAKIRA
8	CAMERON DIAZ
9	SALMA HAYEK
10	SOFIA VERGARA

2012  
EMMA WATSON

# Sophisticated Phishing Chain



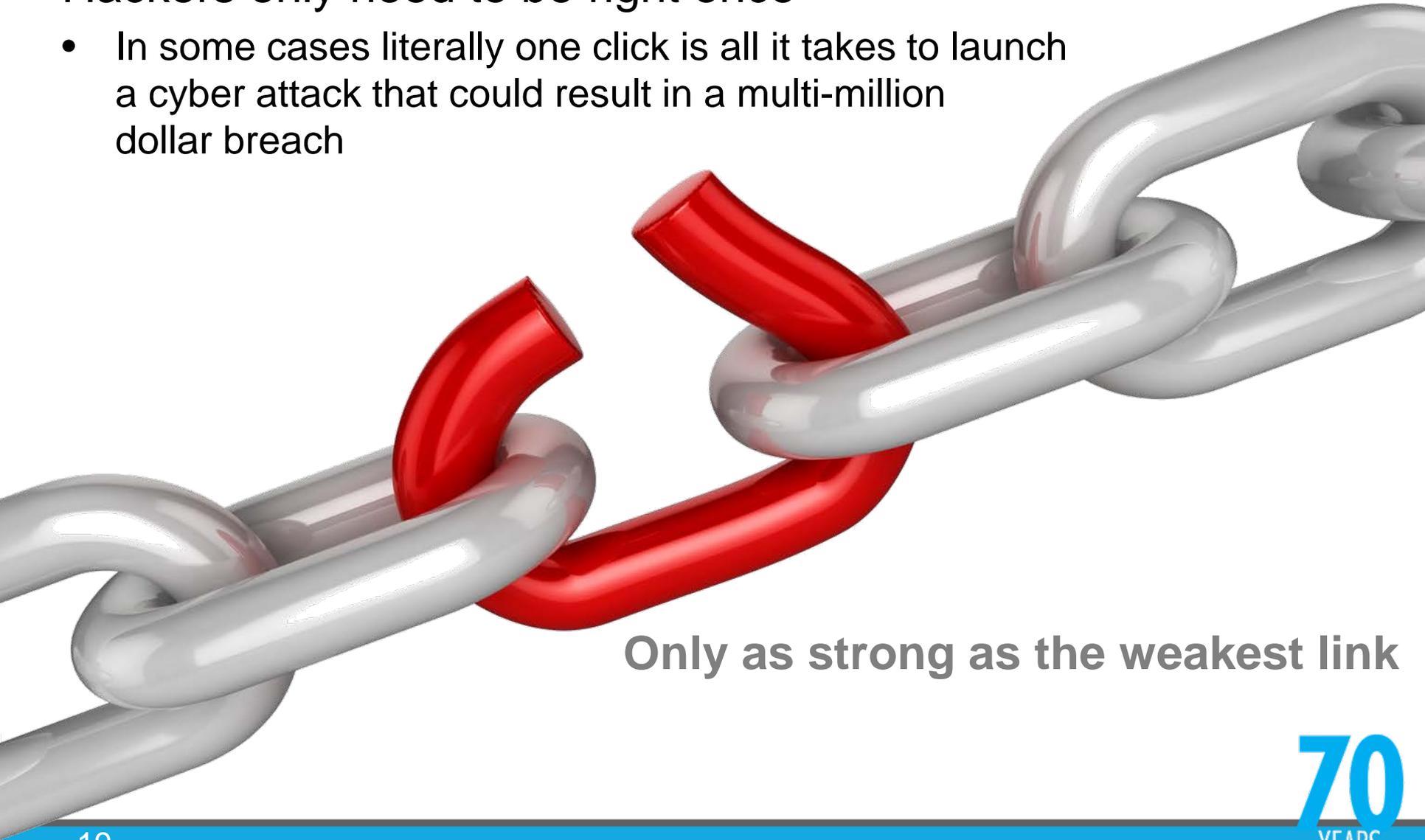
Professional, methodical approach to steal data:

- 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

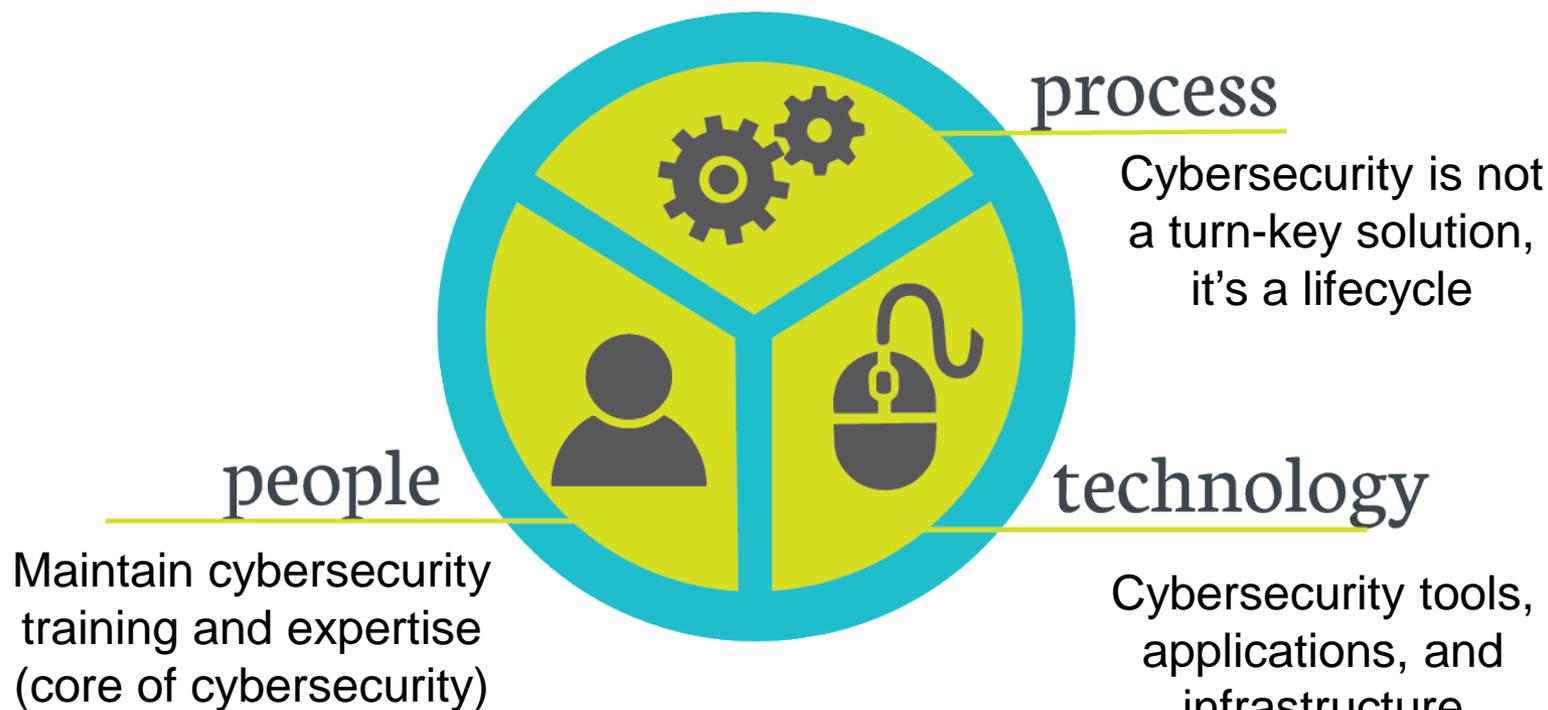
# Cybersecurity Realities, Cont.

- 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



# Cybersecurity Realities, Cont.

Comprehensive cybersecurity solutions must involve a combination of investments



**Cybersecurity is a ongoing commitment**

# MERS Cybersecurity Risk Mitigations

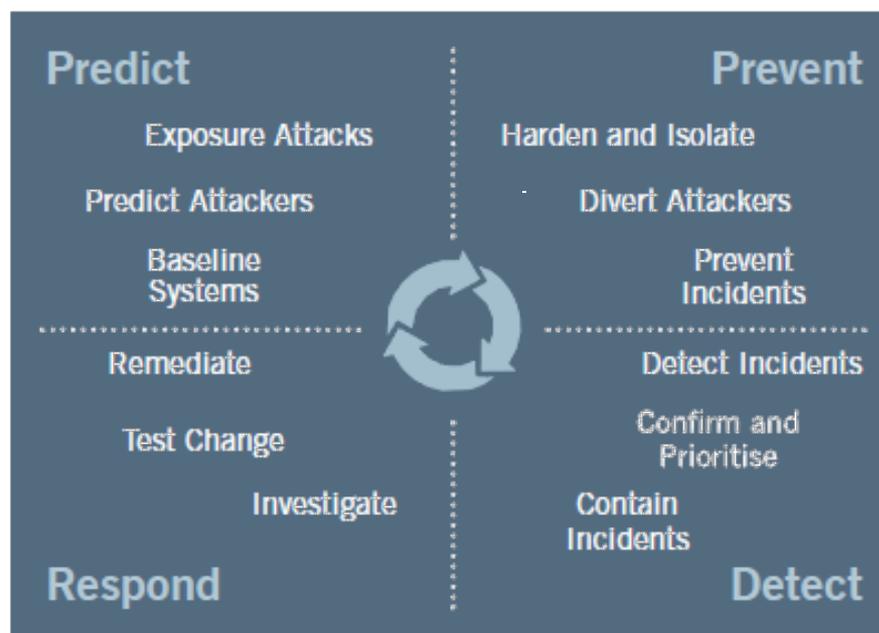
---

- 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

# 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	
12 char	16	40 days	212k years	20m years	970n years	2tn years
		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

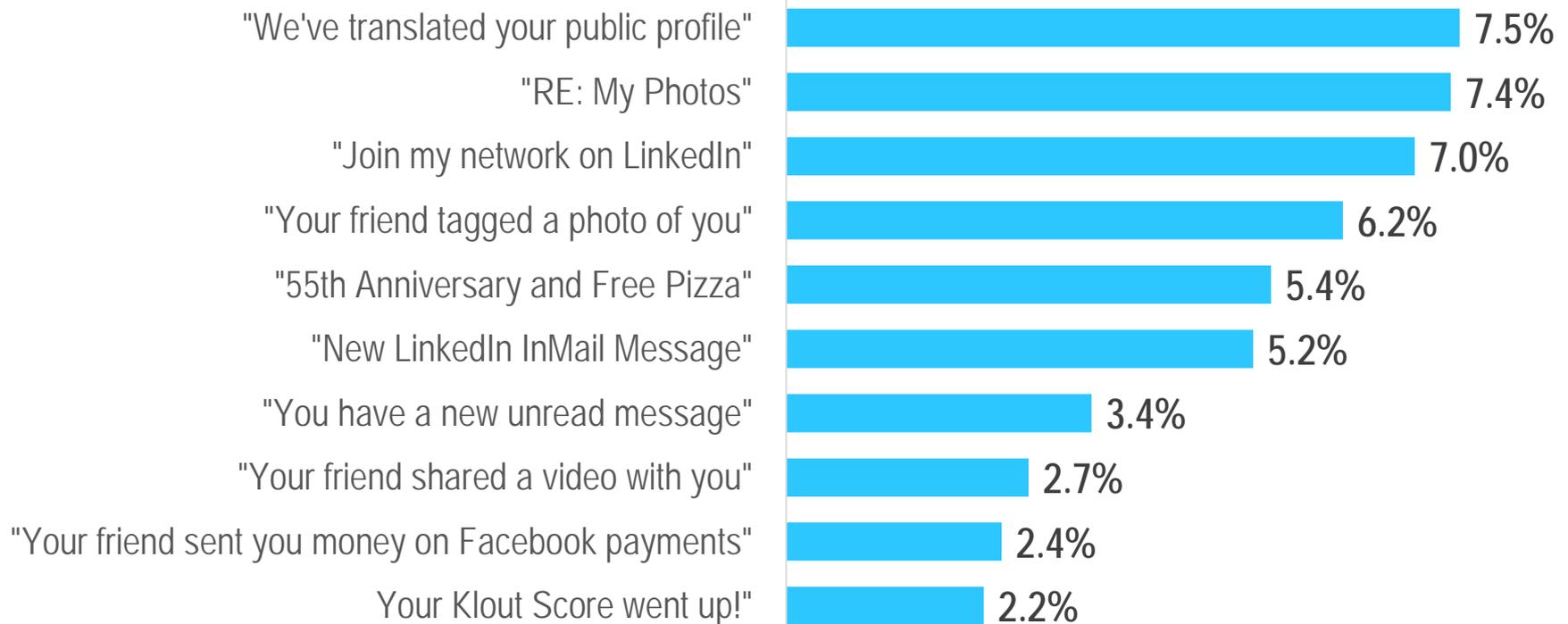
Twitter has 294  
million active  
users

LinkedIn has  
187 million  
active users

# Common Social Media Scams

This year's most clicked social media scam lines

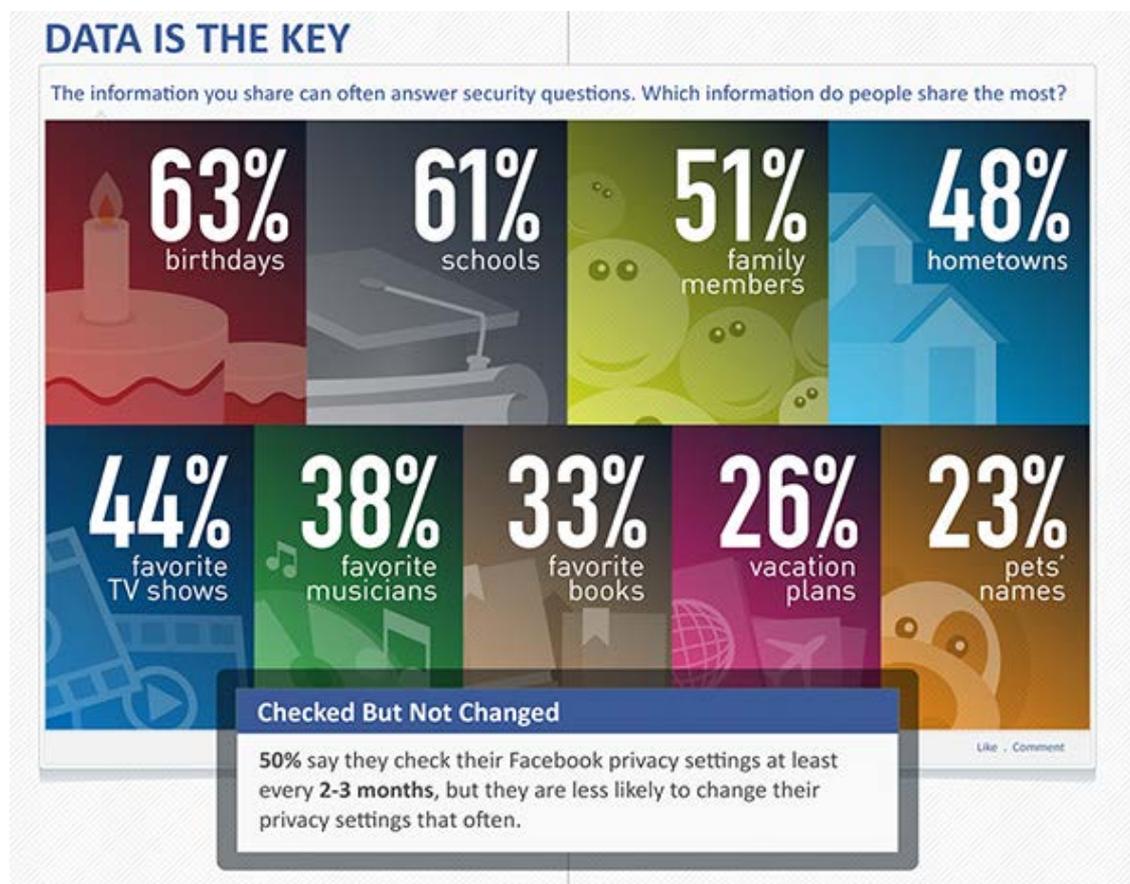
% THAT CLICKED



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



# 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



# 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!***

# Contacting MERS

---

MERS of Michigan  
1134 Municipal Way  
Lansing, MI 48917

*Phone: 800.767.6377*  
*[www.mersofmich.com](http://www.mersofmich.com)*

**LET'S GET SOCIAL!**

