



Social Threats – Social Media as an Attack vector for Cyber Threats

Stewart Cawthray

General Manager, Enterprise Security Products &
Solutions

April 26, 2017

#WHOAMI

- **General Manager Security Products – Rogers Enterprise**
- 15 Year **Security Veteran**
- **Industry Speaker** & Cybersecurity Evangelist
- Devoted Father & Field Hockey Coach
- Twitter: **@StewartCawthray**





#WhatWeDo

Rogers Security Services

Enterprise Cybersecurity Protection for Businesses of All Sizes

THE SOCIAL REVOLUTION

GLOBAL SCALE OF SOCIAL MEDIA

95%

US WORKING AGE ARE **ACTIVE** ON
SOCIAL MEDIA

3/4

WORLDWIDE INTERNET USERS
HAVE **ACTIVE** SOCIAL PROFILES

IMPACT ON DAILY LIVES

27%

INTERNET TIME SPENT
ON SOCIAL MEDIA

3 HOURS

EVERY **DAY** SPENT ON
SOCIAL MEDIA

■ IMPACT ON ECONOMY

50%

OF AMERICAN'S LEVERAGE
FACEBOOK FOR PURCHASE
DECISIONS

25%

IS **PINTEREST'S** SHARE OF
INTERNET RETAIL REFERRAL
TRAFFIC



SOCIAL MEDIA

THE BUSINESS PLATFORM



SOCIAL CREATES BUSINESS VALUE

MARKET PERFORMANCE FOR BRANDS
CREATING VALUE THROUGH
SOCIAL VS. S&P 500



40% Increase in performance for social brands vs. S&P 500

60% buying decisions made on perception of brand vs. product or service quality

MASSIVE INVESTMENT INTO SOCIAL

Enterprise CMOs to spend **10.8%** of marketing budget on social in next 12 months growing to **22.4%** in five years.

57.5% are worried that use of online customer data could raise questions about privacy.





YIKES!

SOCIAL MEDIA CAN BE
DANGEROUS

IT'S ALL OVER THE NEWS

\$100 JCPenney Coupon Scam

Scammers attempt to lure Facebook users into believing they can get a \$100 JCPenney coupon for liking and sharing a post.

Forbes / Tech

AUG 24, 2014 @ 10:49 PM 54,671 VIEWS

Hackers Ground Sony Executive's Flight With Bomb-Threat Tweet

Chipotle apologizes for racist tweets during Twitter hack

HACKED: A C

August 18, 2015 Uncategorized

SOCIAL MEDIA

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING

Twitter CFO's account hacked

Ben Berkowitz | @BerkowitzBT

Tuesday, 10 Feb 2015 | 2:19 PM ET

CNBC

Delta Airlines a

rated Facebook

An obscene headline and wel

Instagram has a problem it need

lead to exploit kits so they c

By: Ankit Singh SYMANTEC EMPLOYEE

Created 22 Jul 2014

Checkpoint

U.S. military social media accounts apparently hacked by Islamic State sympathizers

APT 29 use Twitter to control its Hammertoss data stealer

July 31, 2015 By Pierluigi Paganini

G+1 10

f My Page

f Like 56

Experts at FireEye discovered a new APT group dubbed APT 29 that is exploiting Twitter to mask the activities of their data-

OFFICIAL SECURITY BLOG

Malwarebytes
UNPACKED

Home Authors Videos Scams About Us Archives + Categories + Q

Fake Twitter Verification Profile leads to Phishing, Credit Card Theft


JUNE 30, 2015 | BY CHRISTOPHER BOYD



AND IT'S NOT HYPE


CISCO
FACEBOOK SCAMS
ARE THE **#1** WAY
TO **BREACH**
THE NETWORK


EMPLOYEES EXPERIENCE
CYBERCRIME
ON **SOCIAL**
MEDIA MORE THAN
ANY OTHER
BUSINESS PLATFORM

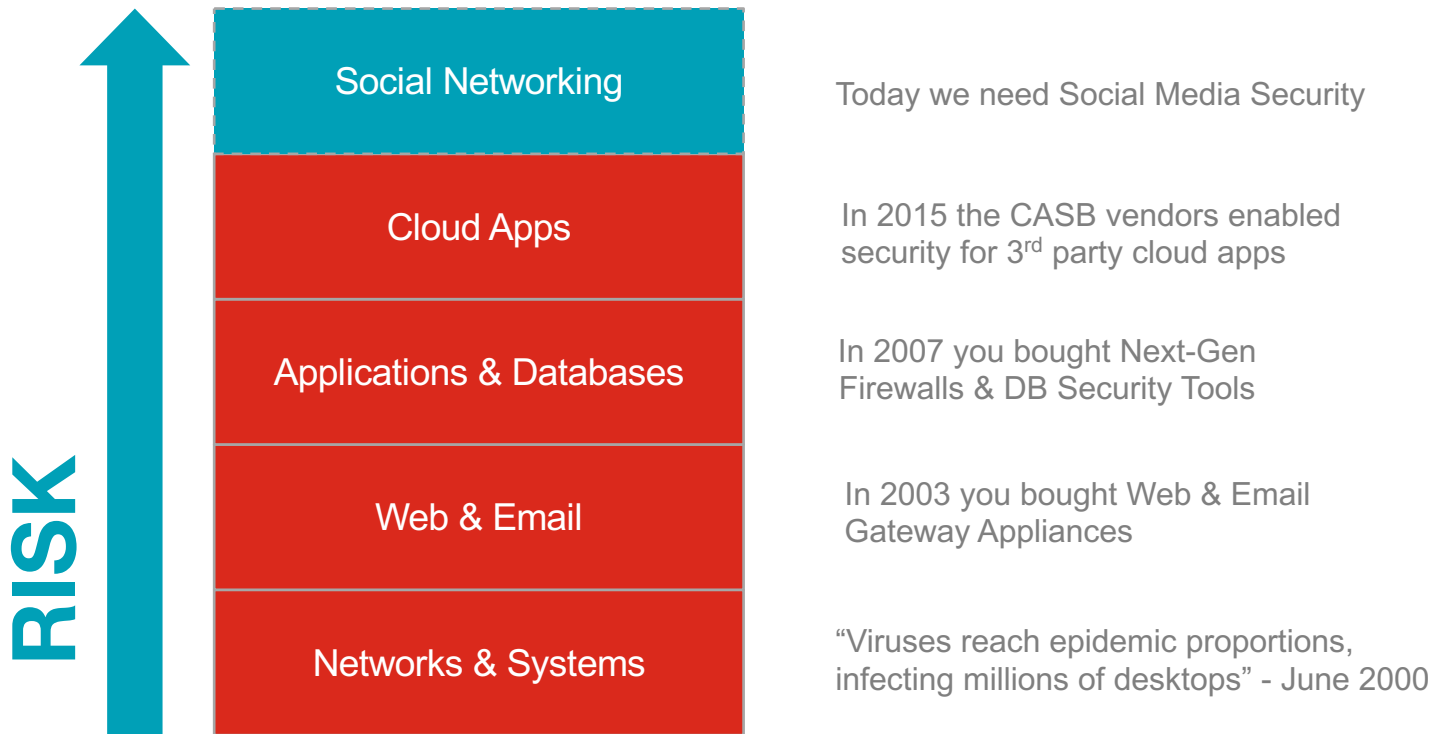

OF ALL SOCIAL USERS
92% REPORT RECEIVING **SPAM**
54% REPORT RECEIVING **PHISHING LINKS**
23% REPORT RECEIVING **MALWARE**
1 IN 5 HAVE BEEN **HACKED**


29 MILLION
TWEETS
EVERY DAY
ARE MALICIOUS

 | **160,000** facebook ACCOUNTS BREACHED EVERY DAY

  | YEARLY COST OF SOCIAL MEDIA PHISHING **\$1.2 BILLION**

TIME TO TREAT SOCIAL AS A RISK SURFACE



THE PROBLEM WITH SOCIAL

BUSINESS RISKS

- External **Fraud** & Customer **Data Loss**
- Impersonations & **Reputation Damage**
- **Counterfeit**, Piracy & **Trademark** Usage

“Due to the amplification effects of social media, [reputational risk] operational losses can greatly exceed the value of the physical loss from a risk event.”

Gartner

SECURITY THREATS

- Targeted Attacks & **Social Engineering**
- **Insider Threat** & Data Loss
- **Executive Protection** & Threat Intelligence

“Social media scams are the #1 method to breach the network, far more common than traditional email phishing, and Facebook is the #1 source of malware.”

CISCO

**DO YOU
HAVE
VISIBILITY?**

ANATOMY OF AN ATTACK: ENTERPRISE SOCIAL MEDIA

TARGET

WHY / IMPACT

TACTICS

EMPLOYEES

Humans are compromised in order to bypass security defenses and gain access to “protected” systems and sensitive data



HASHTAG HIJACKING



ACCOUNT TAKEOVER



IMPERSONATIONS



ATTACK PLANNING



SOCIAL PHISHING



SOCIAL ENGINEERING



INFORMATION LEAKAGE

BUSINESS OPERATIONS

Sensitive, confidential & protected information is published & malicious actions coordinated to damage revenue generating activities & biz trust

CUSTOMERS

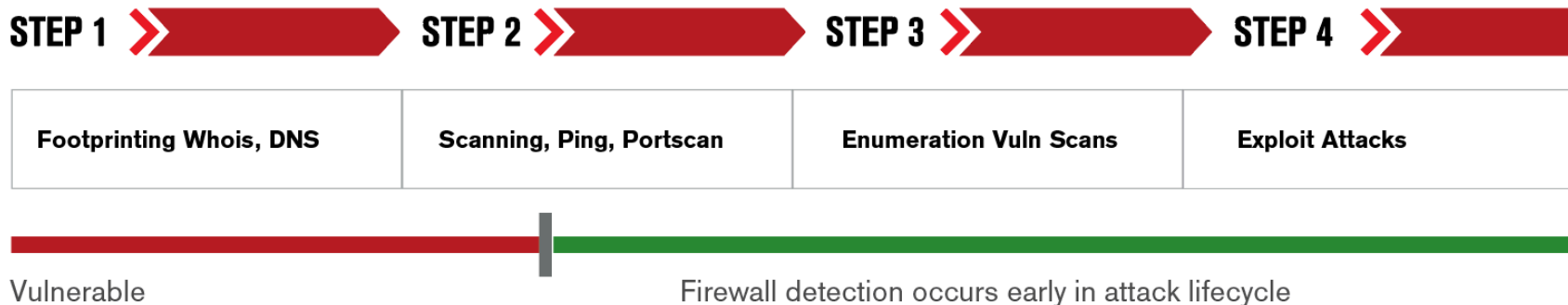
Customers are targeted through fraudulent impersonations of the org and key executives to steal customer data & damage reputation

SOCIAL MEDIA THREAT LANDSCAPE

- ***Social media blurs the lines*** between our personal lives and work day
- ***New threat landscape*** is evolving introducing new methods of attack
- **Social media attacks are being used to:**
 - ✓ Impersonate executives, brands, and employees
 - ✓ Hijack Accounts
 - ✓ Distribute malware
 - ✓ Phish credentials
 - ✓ Discredit company brands
 - ✓ Perform scams
 - ✓ Execute cyber attacks
 - ✓ Stage violence
 - ✓ And more...

TRADITIONAL NETWORK ATTACK VS. SOCIAL MEDIA ATTACK

TRADITIONAL NETWORK ATTACK



SOCIAL MEDIA ATTACK – BUILD A NETWORK OF TRUST

SOCIAL MEDIA NETWORK ATTACK



Build a network of “trust”!!!

FOOTPRINT

LinkedIn	company employees, titles, locations, email addresses, phone numbers, former employees
Twitter	bio, interests, other Twitter accounts they own, other brands/sub-brands, employees responsible for managing brand accounts, followers
Facebook	bio, birthday, interests, hobbies, connections
Google+	corporate ID or login, interests, hobbies, connections

MONITOR & PROFILE

- **Social Media Accounts**
- **Dormant accounts**
- **Subsidiaries**
- **Responsible people for those accounts**
- **Partners**
- **Keywords**
- **#Hashtags**
- **@<mentions>**
- **\$Stock**
- **Hobbies, interests**
- **Titles**



IMPERSONATIONS

- Sampling of approximately **100 enterprises shows more than 1000 impersonation accounts are created weekly** by perpetrators.



- Attackers creating homoglyph spelling of handles, name, and bio.
- Image analysis can identify identical or photoshopped images

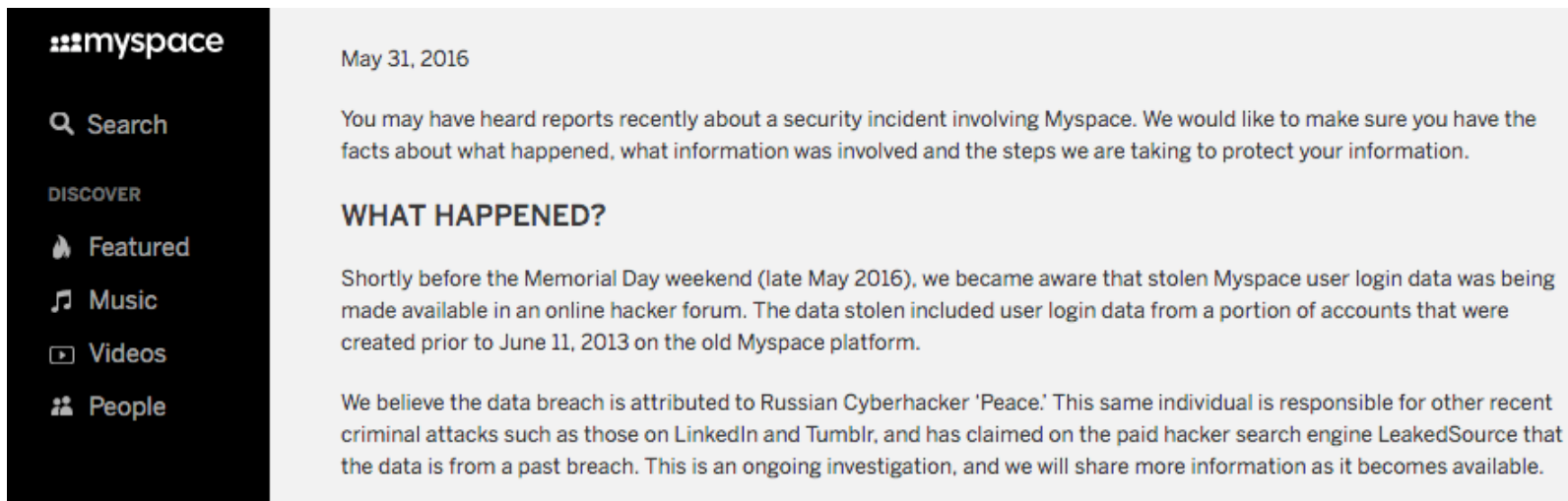
IMPERSONATIONS – ENTICE FOLLOWERS AND CONNECTIONS

- @<mentions> of targets
- #hashtags common to targets
- Keywords targets use
- Follow targets
- Further campaign



HIJACKING – HOW?

- Reuse of exposed passwords on other social networks



The screenshot shows the Myspace website interface. On the left is a dark sidebar with the Myspace logo and navigation links: Search, DISCOVER, Featured, Music, Videos, and People. The main content area is light gray and contains a date stamp 'May 31, 2016', an introductory paragraph about a security incident, a section titled 'WHAT HAPPENED?', and two paragraphs of text explaining the breach and the company's response.

myspace

Search

DISCOVER

Featured

Music

Videos

People

May 31, 2016

You may have heard reports recently about a security incident involving Myspace. We would like to make sure you have the facts about what happened, what information was involved and the steps we are taking to protect your information.

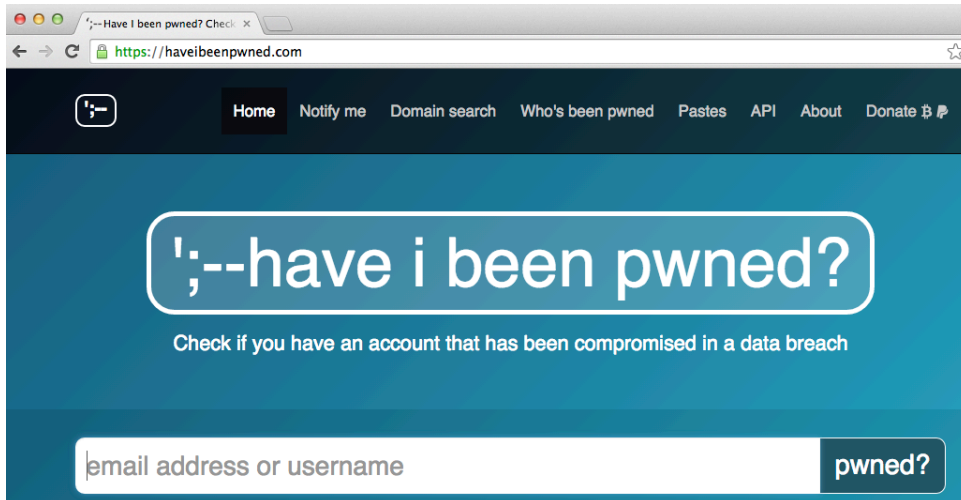
WHAT HAPPENED?

Shortly before the Memorial Day weekend (late May 2016), we became aware that stolen Myspace user login data was being made available in an online hacker forum. The data stolen included user login data from a portion of accounts that were created prior to June 11, 2013 on the old Myspace platform.

We believe the data breach is attributed to Russian Cyberhacker 'Peace.' This same individual is responsible for other recent criminal attacks such as those on LinkedIn and Tumblr, and has claimed on the paid hacker search engine LeakedSource that the data is from a past breach. This is an ongoing investigation, and we will share more information as it becomes available.

HIJACKING – HOW?

- Other sources of possible passwords on Social Web (Pastebin, Troy)



ATTACK METHODS – Tactics Techniques Procedures

- **Establishing trust** is fundamental
- Without connections, followers, or friends; the attack surface is limited
- **Connected targets increases the success of an attack** and compromise
- Social Media automates **shortened URLs**
- While a benefit to social media in general, it also allows attackers to **obfuscate** malicious and phishing URLs
- We can also reverse footprint social media URL security and serve good/bad content based on this

ATTACK METHODS – URL SHORTENERS

- Shortened URLs come in many forms:

Company	Legitimate Shortened URL
Bitly	bit<dot>ly
Google	goo<dot>gl
Hootsuite	ow<dot>ly
TinyURL.com	tinyurl<dot>com
Tiny.cc	tiny<dot>cc

- Many (but not all) do not check for bad URLs

ATTACK METHODS – OBFUSCATED MALICIOUS URL

ALERT DETAILS



Retweets: 2

RT @fondieuropei20: #PMI #innovazione
Macchinari ed emozioni, la rivoluzione umana

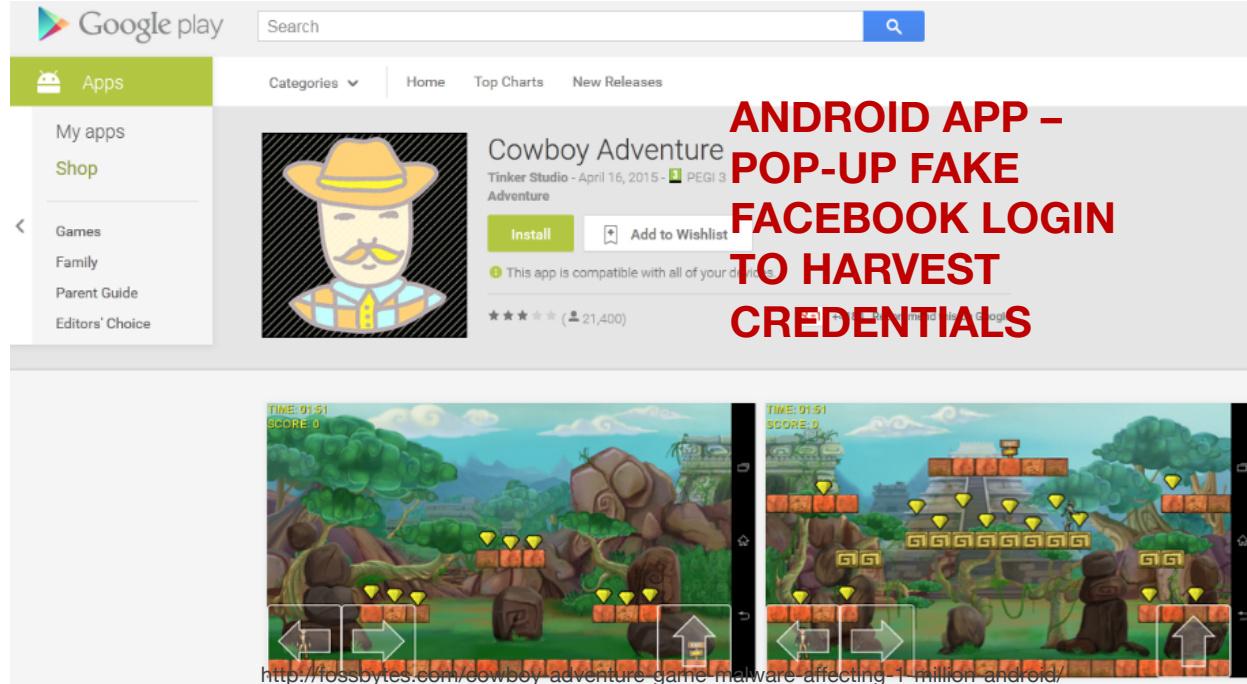
di Techshop - La Stampa <http://bit.ly/1XEN5li>

Destination URL: <http://3488fns.com/c/d?i=4lIZaBKQyam>

>> View Offending Content Source

ATTACK METHODS – MALICIOUS URLs

- Malware
- Phishing Link
- Malicious Browser Plug-in
- Bad App



ATTACK METHODS – MALICIOUS ADVERTISING

Creative Audience Optimization & Pricing

Audiences

Use Existing Targeting Group

Custom Audiences

My Roommate x

Excluded Audiences

Enter a custom audience to exclude

Location

Add a country, state/province, city or ZIP

Age

Any — Any



Trouble swallowing pills?

gallery.zzq.org

Does it seem ironic that swallowing swords is easy and then small pills make you gag?

SCAMS, SCAMS & MORE SCAMS



"SPONSORED" SCAMS

Scammers pay Instagram to feature their content to more people

TRADEMARKED IMAGE

Copyrighted content repurposed for malicious activity

BRAND IMPERSONATION

Company name and logo abused to make the scam appear legitimate

CUSTOMER SCAM

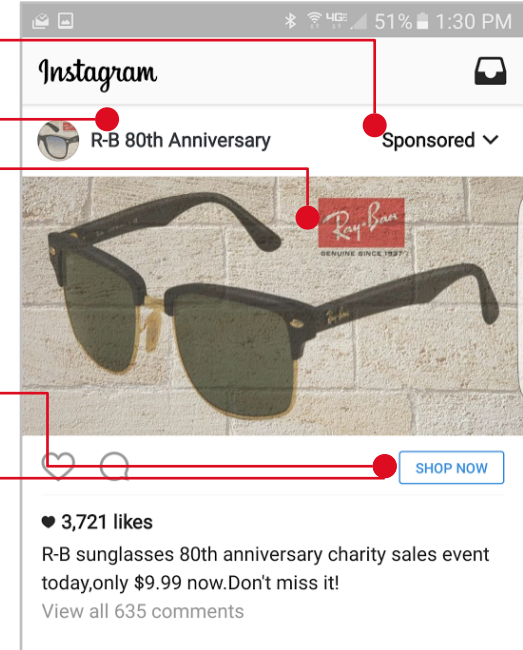
Scam post designed to compromise customer credentials and damage brand

PHISHING LINK

Malicious link redirects to a phishing page intended to harvest credentials

COUNTERFEIT GOODS

Fake good being sold online undermines an organization's bottom line

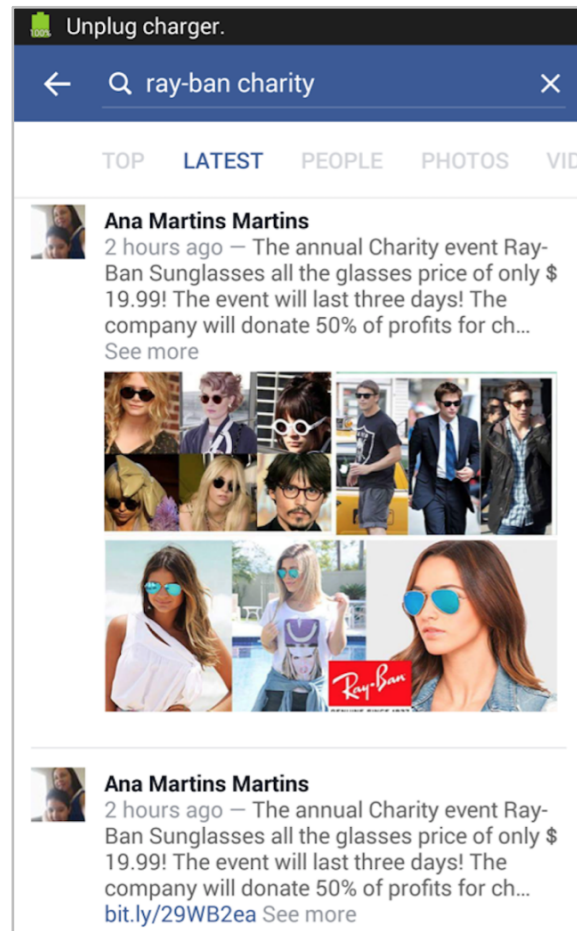


RAY-BAN SUNGLASSES

PHISHING & FRAUD CONTINUE...

CRITICAL ISSUE

- **What:** Fake Ray-Ban Charity Events scams and account hijacking
- **When:** still active... seen activity since at least 2014
- **How:** Fake event offering sunglasses up to 90% off, fools users into purchasing sunglasses through malicious link, also hijacks Facebook account to send event out to more people



RAY-BAN SUNGLASSES

PHISHING & FRAUD CONTINUE...

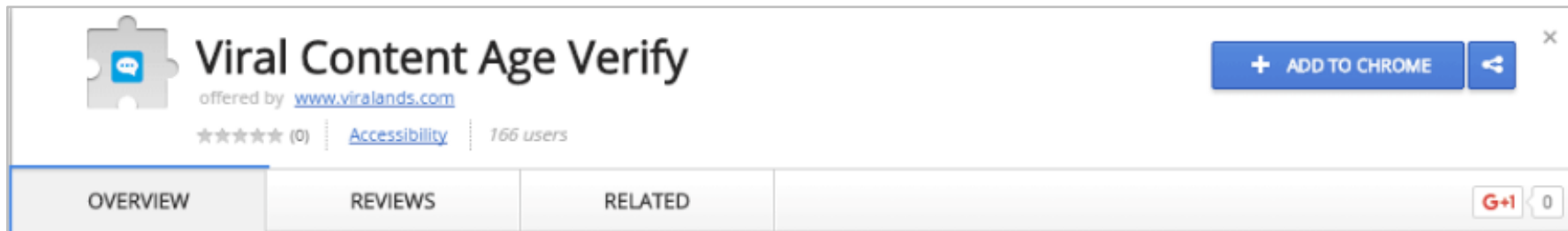
```
      "display_url": "facebook.com/R%D0%B0%D1%83-\u2026",  
      "expanded_url": "https://www.facebook.com/R%D0%B0%D1%83-  
B%D0%B0n-summer-charitable-eventsAll-colors-for-2499-1248946518484005/",  
      "indices": [  
        38,  
        61  
      ],  
      "url": "https://t.co/JljwETzcn0"  
    },  
    {  
      "display_url": "rbvim.com/ray-ban-rb4161\u2026",  
      "expanded_url": "http://www.rbvim.com/ray-ban-rb4161-sur-  
glasses-havana-crystal-frame-brown-polarized-l-p-242.html",
```

FACEBOOK

MALWARE CLICK FRAUD...

CRITICAL ISSUE

- **What:** Facebook malware targets Windows PCs running Chrome browser
- **When:** July 19, 2016
- **How:** User Likes a friend's Liked item, prompts "Verify Age" and install of a malicious Verify Content Age Chrome extension in Chrome store. Downloads a malicious payload, directs user to a malicious page that steals their Facebook (access) tokens



Source: <http://www.scmagazine.com/chrome-browser-extensions-discovered-engaging-in-facebook-click-fraud/article/510843/>

FACEBOOK MESSENGER

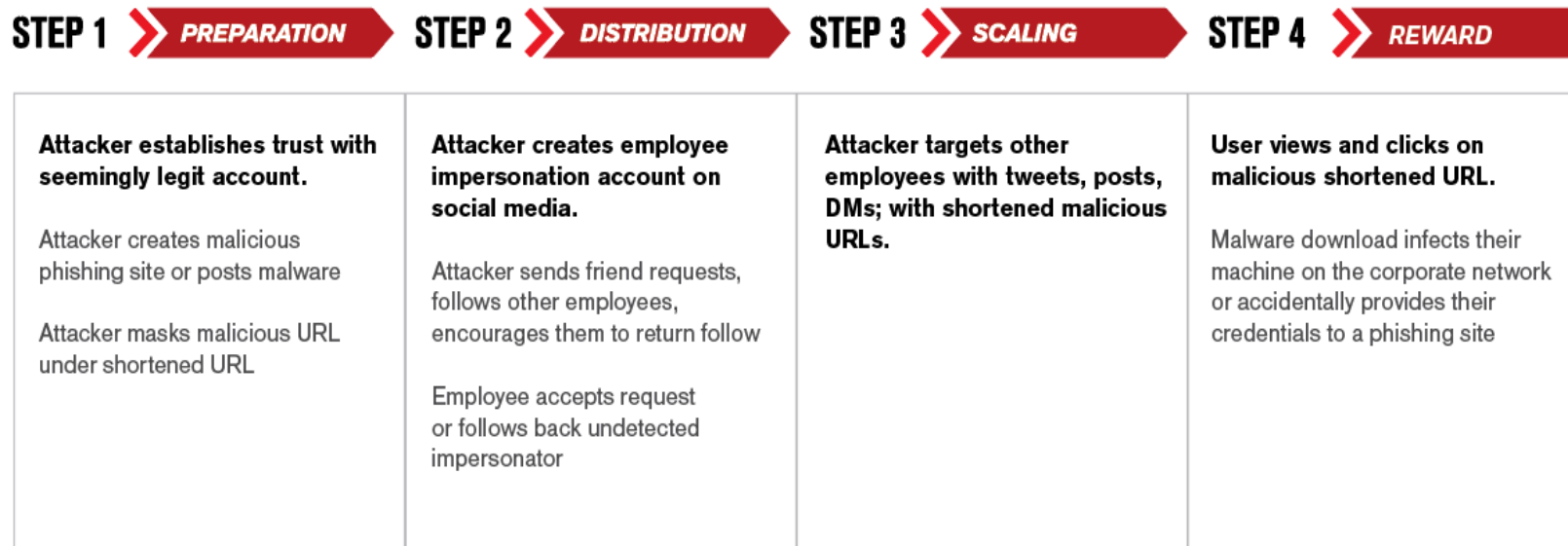
MALWARE...

CRITICAL ISSUE

- **What:** Malware bot targeting Facebook Messenger
- **When:** July 7, 2016
- **How:** User receives a message from a Friend, clicks on link and infects machine (Windows PC with Chrome) with a trojan and hijacks victim's Facebook account and spreads it to other users.

Source: <http://www.digitaltrends.com/computing/facebook-messenger-virus-malware-windows-chrome/>

PUTTING IT ALL TOGETHER



COUNTERMEASURES – FORTIFYING YOUR SOCIAL MEDIA

- **Identify and improve your organization's social media footprint** (companies, accounts, and key individuals)
- **Monitor for impersonation accounts**, and, when malicious, arrange for takedown.
- Enable **two-factor authentication and other settings** for social media accounts to deter hijacking
- Enhance security intel by **feeding social media context**, such as malicious and phishing URLs, into perimeter (firewalls, IDS, MPS, or proxy), endpoint security solutions, and SIEM
- Augment your **incident response plan** and process to encompass social media and include a takedown process.

Introducing Rogers Social Media Security

Confidently leverage social media to enhance your brand and bottom line, while protecting your employees, customers and reputation from cybercriminals.

The first solution of its kind offered by a Canadian telco, Social Media Security:

- Eliminates arduous, ineffective manual searches for threats.
- Effortlessly neutralizes attacks across all major social networks as quickly as possible.
- Is delivered as a fully managed service for a monthly fee included on your Rogers bill.
- Includes 45 days of comprehensive onboarding.



Thank you!

An aerial photograph of a city skyline at sunset. The sun is low on the left, creating a bright lens flare and illuminating the clouds. The city features various skyscrapers, including a prominent tall, thin one on the right. A network of thin white lines connects several points across the city, including the tall skyscraper and a large circular building in the foreground. The text "Your success is our business." is centered in a white serif font.

Your success is our business.

