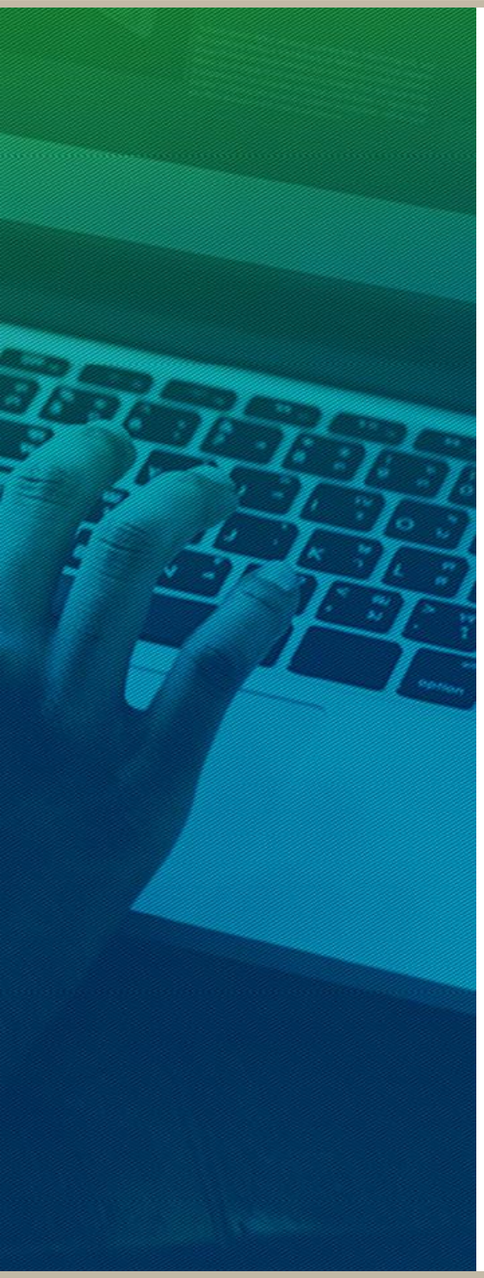
Prevent Cyber Attacks
Canadian Home Builders Assocaition

MNP Cyber Security Presentation

Presented by:
Danny Timmins, National Cyber Security Leader
November 2017

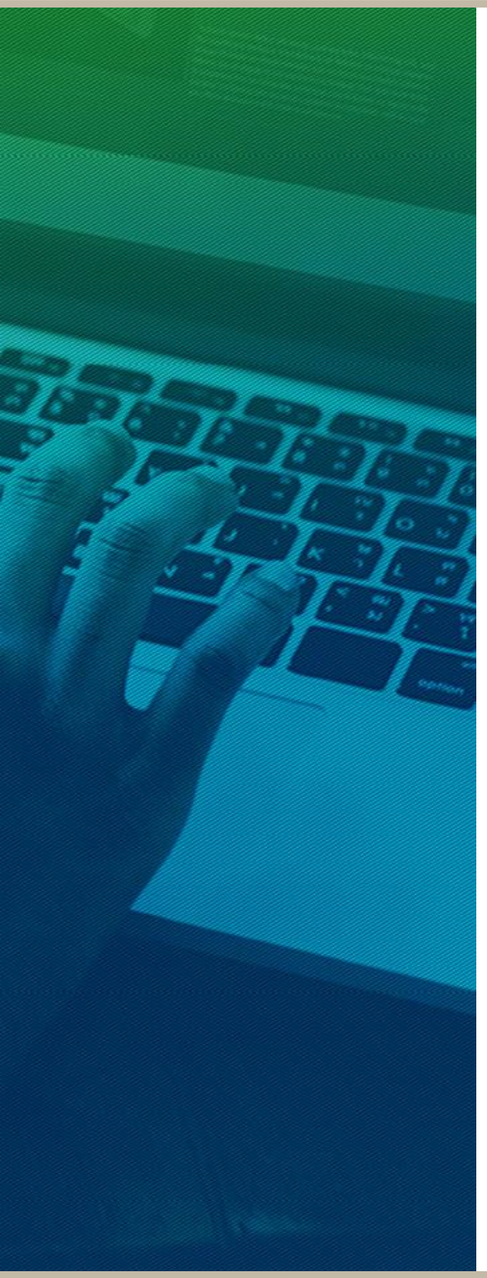
Cyber Security › **MNP Technology Solutions**



- **Cyber Security Overview**
- **Cyber Crime Tactics and Techniques**
  - Hacking (Penetration Testing)
  - Social Engineering (Malware/Crimeware)
  - Red Teaming
- **Considerations**

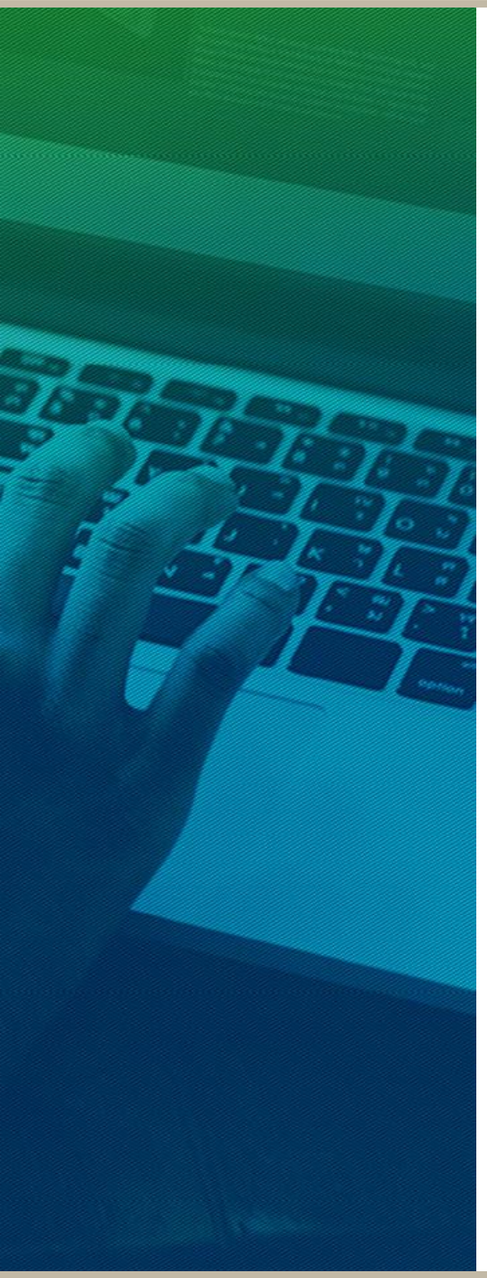
Lessons from the field

- Canada’s 5th Largest Accounting | Tax | Consulting
- 4500 Team Members
- 80 Offices coast to coast
- 55 Cyber Security Professionals Nationally



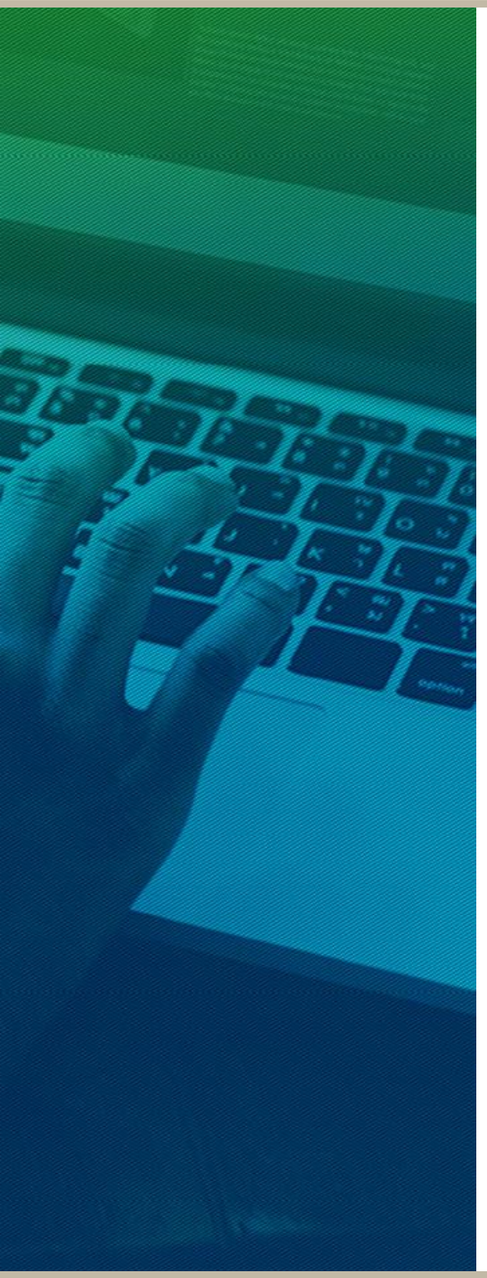
MNP is more than an Accounting Firm

- Digital Strategy
- Portal Development
- Business Continuity
- Workplace Collaboration
- CRM/ERP
- Cloud Strategy
- Operational Technology
- IoT
- Cyber Security & Risk
- Data Analytics
- DevOps
- Auditing



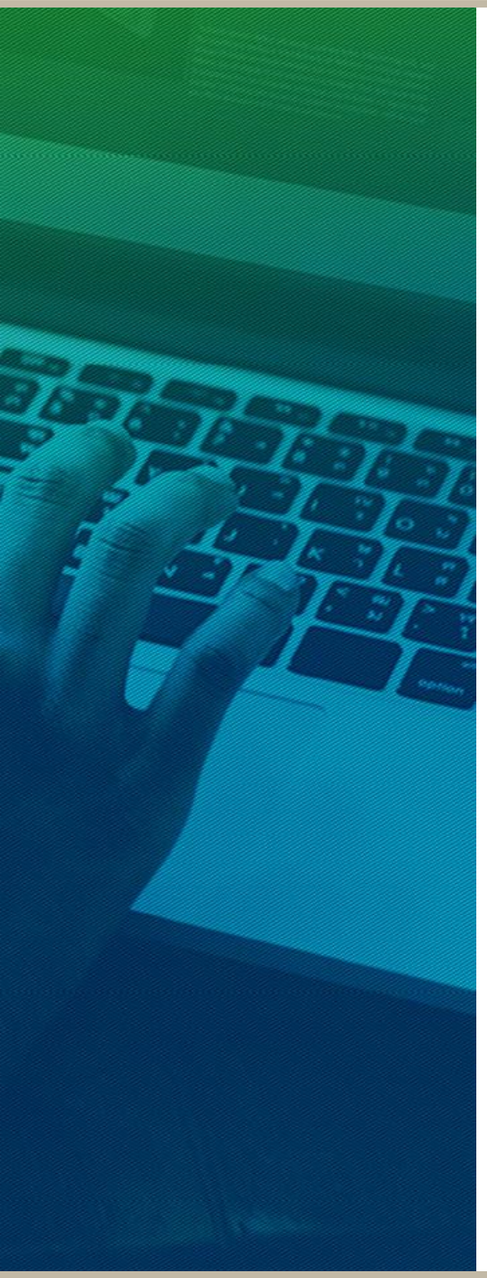
Predictions

- 99% of vulnerabilities exploited will continue to be the ones known by security/IT professionals.
- The single most impactful enterprise activity to improve security will be patching.
- The second most impactful enterprise activity to improve security will be removing web server vulnerabilities.



Predictions

- Internet of Things will grow to an installed base of 20.4 billion.
- A third of successful attacks experienced will be on their shadow IT resources.
- Companies are using more than 15 times more cloud services to store critical company data than CIOs were aware of.
- Nearly eight in ten (77%) of decision makers admit to using a third-party cloud application without approval.



What's happening…

Canada's new privacy laws will require breach notice and affect private sector operations in Canada. (Digital Privacy Act)…do you know how safe your client data is?

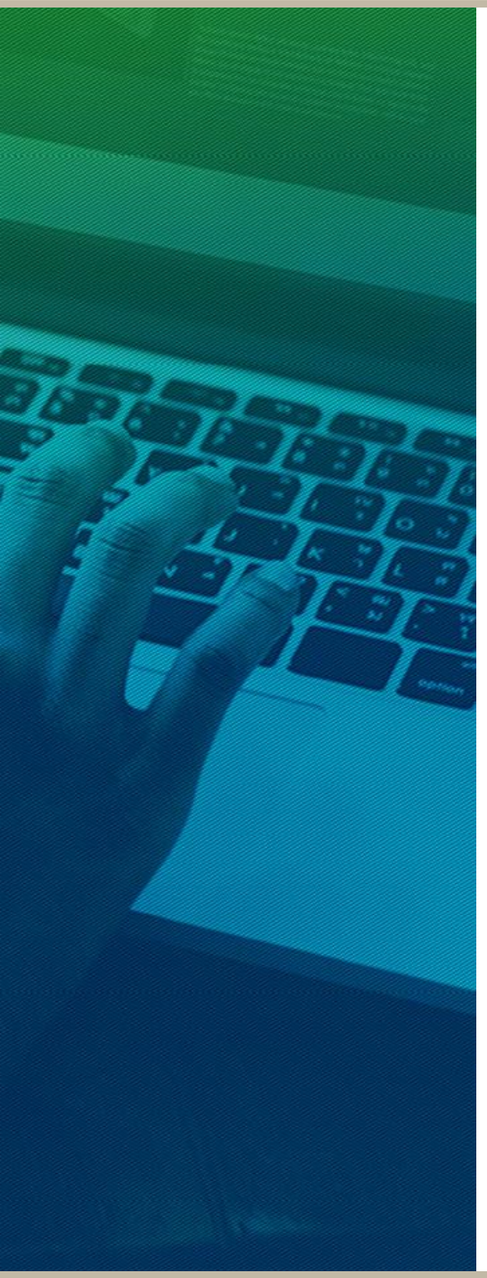
Canada's privacy watchdog planning to pro-actively investigate companies

Excerpt: Canada's privacy watchdog is transforming the way it has pursued protective measures for more than 15 years, planning to more actively go after companies and other organizations for privacy concerns. And it has renewed calls for an update t... Show more

Canada's privacy watchdog planning to pro-actively investigate companies

Commissioner Daniel Therrien also repeated his call for changes to federal law that would give his office the ability to issue orders and

Like Comment | 16 1

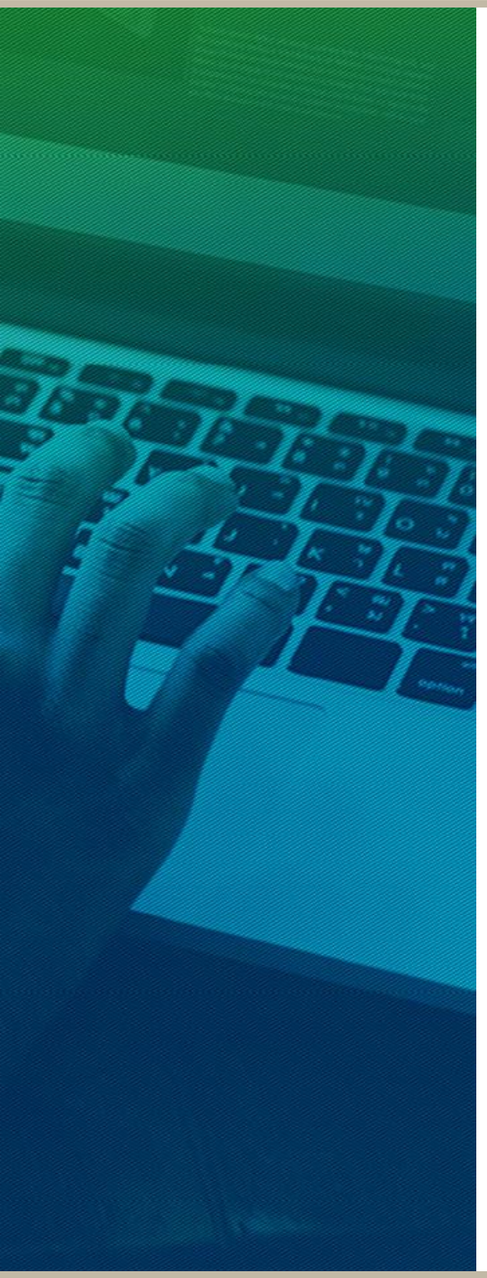


What's happening in the industry?

Damages have started to increase in Canada – Class Action Suits are here - Casino Rama is an example ….30+ Million

Cyber Insurance…how much do you need …is it focused on the correct areas?


thestar.com
Business
Threat of cyberattacks ‘more worrisome than all the other stuff’: Bank of Canada governor
Stephen Poloz shared his unease at a time when governments, central banks and the private sector around the world are searching for new strategies to counter hacks.

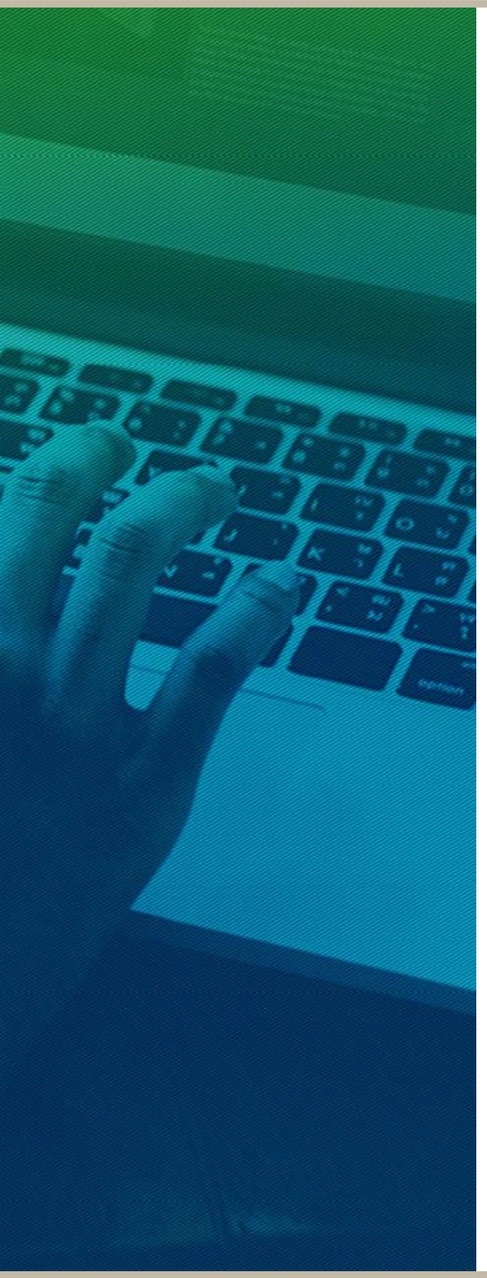


What's happening in the industry?

Mandatory cyber audits coming for publicly traded companies in Canada…. US is pushing hard – its coming

Payment Card Industry (PCI) already has compliancy. IE: Best Western Motels - have been targeted-very limited security

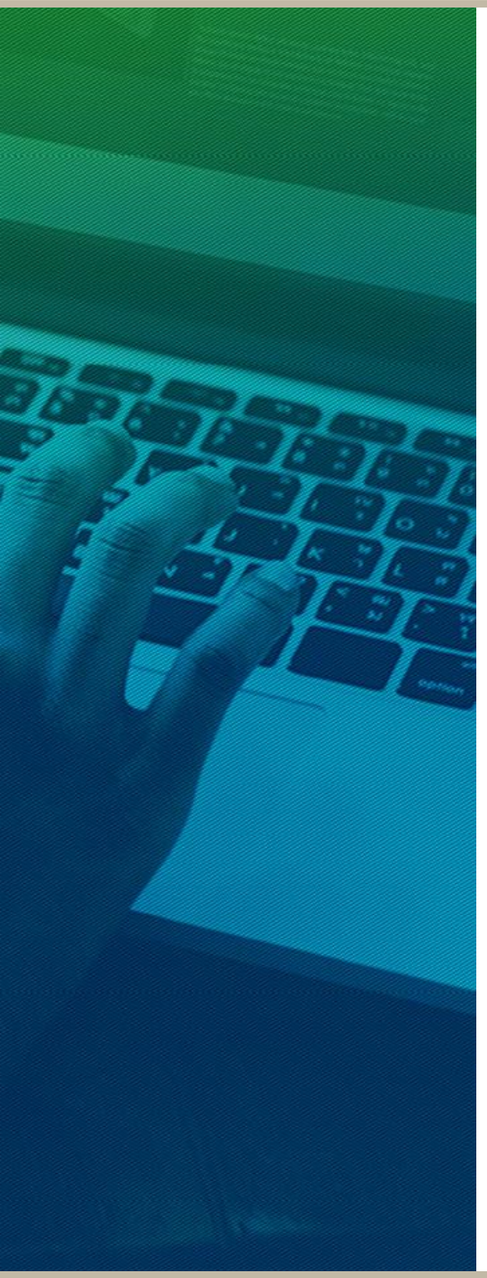
Equifax 140M plus - 100+ thousand in Canada….patch management said to be the issue…mishandled from the start of the breach…directing clients to a phishing site



Who are Behind Cyber Attacks?

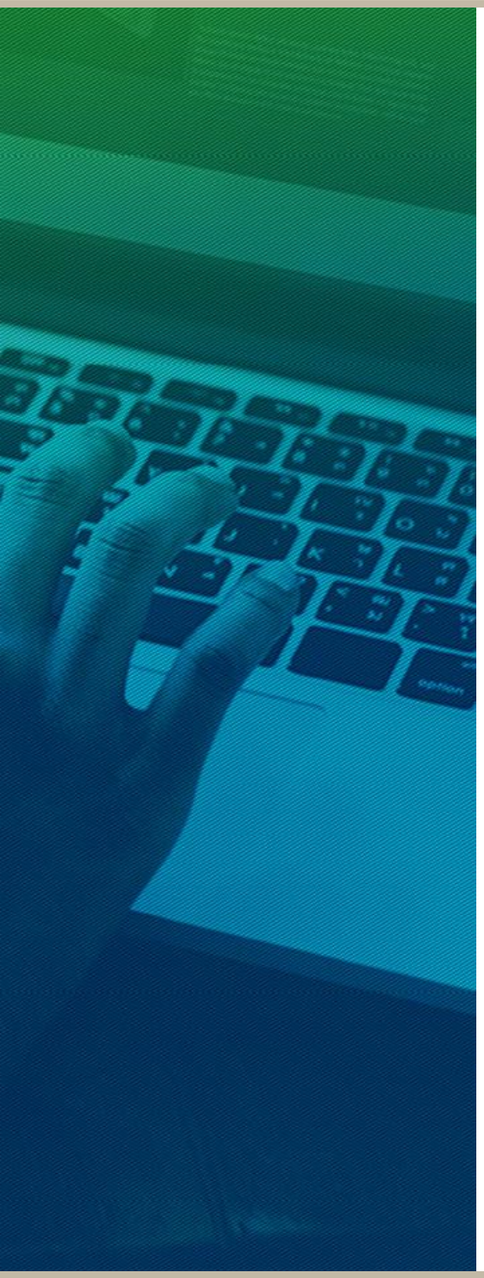
- **Nation States**
- **Organized Hackers**
- **Non-Organized Hacker**
- **Employee: Technical**
- **Employee: Business**
- **Malicious Former Employee**

***89% of breaches had financial or espionage motive*



Some Risks to Consider

- Brand and reputation
- Unable to fulfill service commitments
- Strategic plans, engineering drawings, RFP’s, Proposals, etc.
- Supply Chain/Vendor Management
- New Automation deployments - IoT (Internet of Things)
  - Life Safety Systems – automated systems, elevators, exhaust
- Privacy - Personal Identification Information (PII)
- Regulator Compliance
- Intellectual Property (IP)
- Payment Systems (Ecommerce or Point of Sale)



Cyber-attacks have:

- Disrupted businesses
- Resulted in financial losses
- Tarnished organizations' reputations
- Destroyed careers

Who's making the decisions

JUL 13, 2015 @ 01:42 PM 11,527 VIEWS

Why Cybersecurity Leadership Must Start At The Top

Frontline, CONTRIBUTOR

Dispatches on Cybersecurity FULL BIO

Opinions expressed by Forbes Contributors are their own.

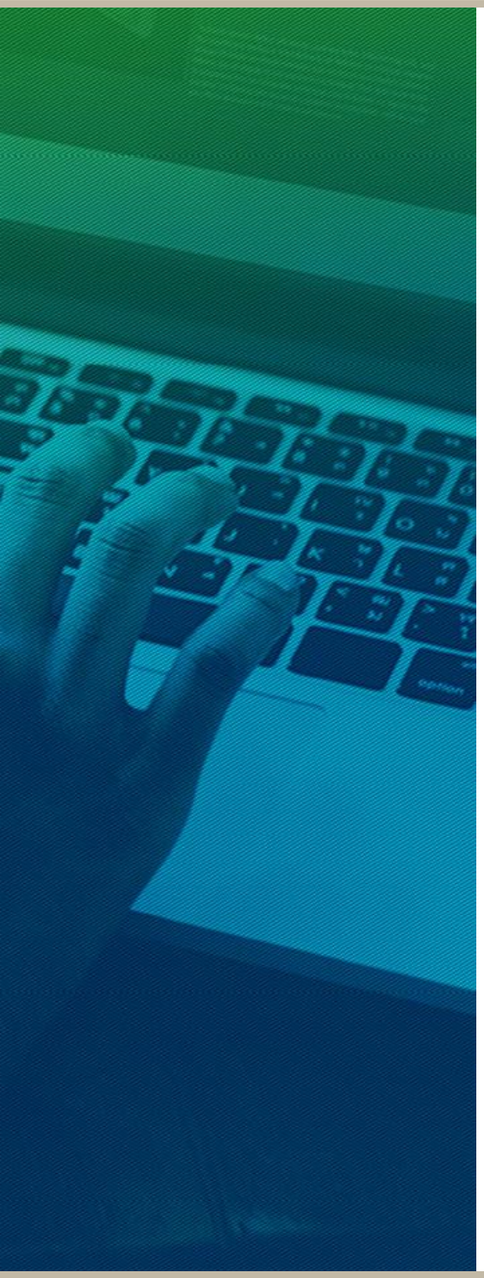
JUL 1, 2016 @ 04:21 AM 7,294 VIEWS

It's Time To Think Of Cybersecurity As A Business Enabler

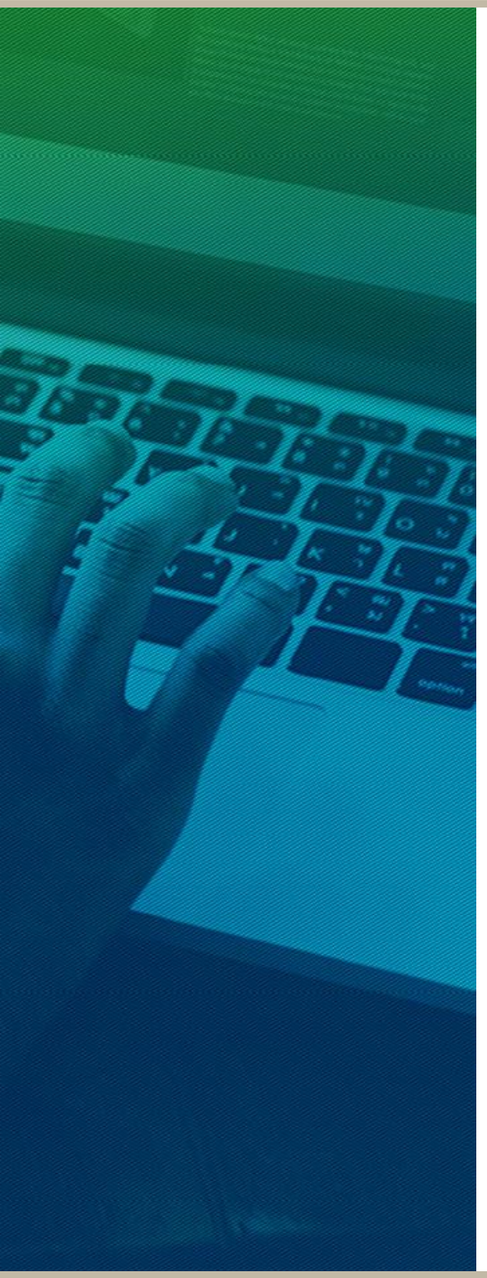
William H. Saito, CONTRIBUTOR

I write about cybersecurity, innovation & Japan. FULL BIO

Opinions expressed by Forbes Contributors are their own.

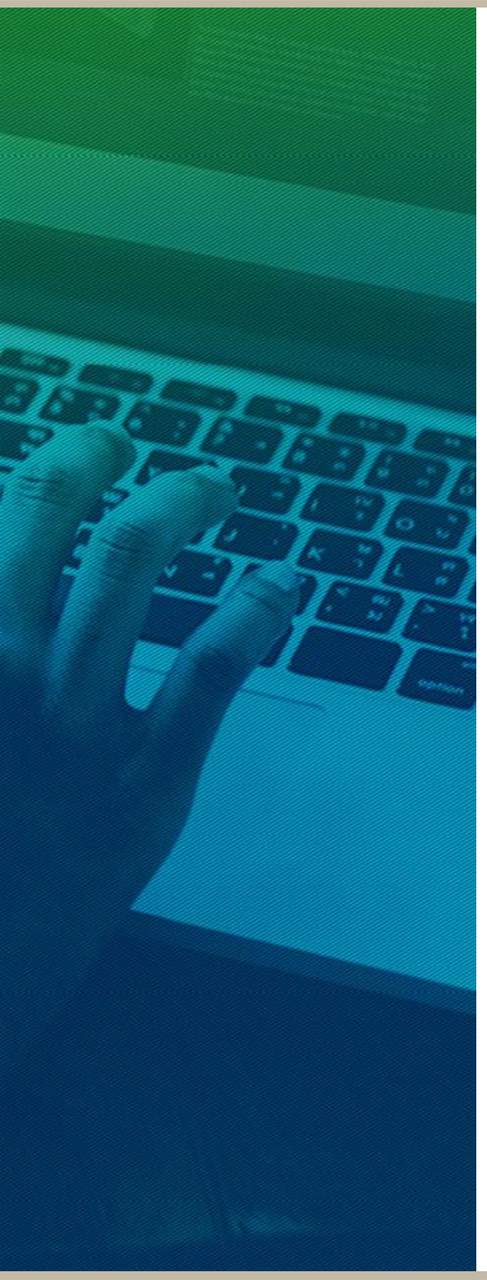


Let’s take a closer look!



What is Hacking?

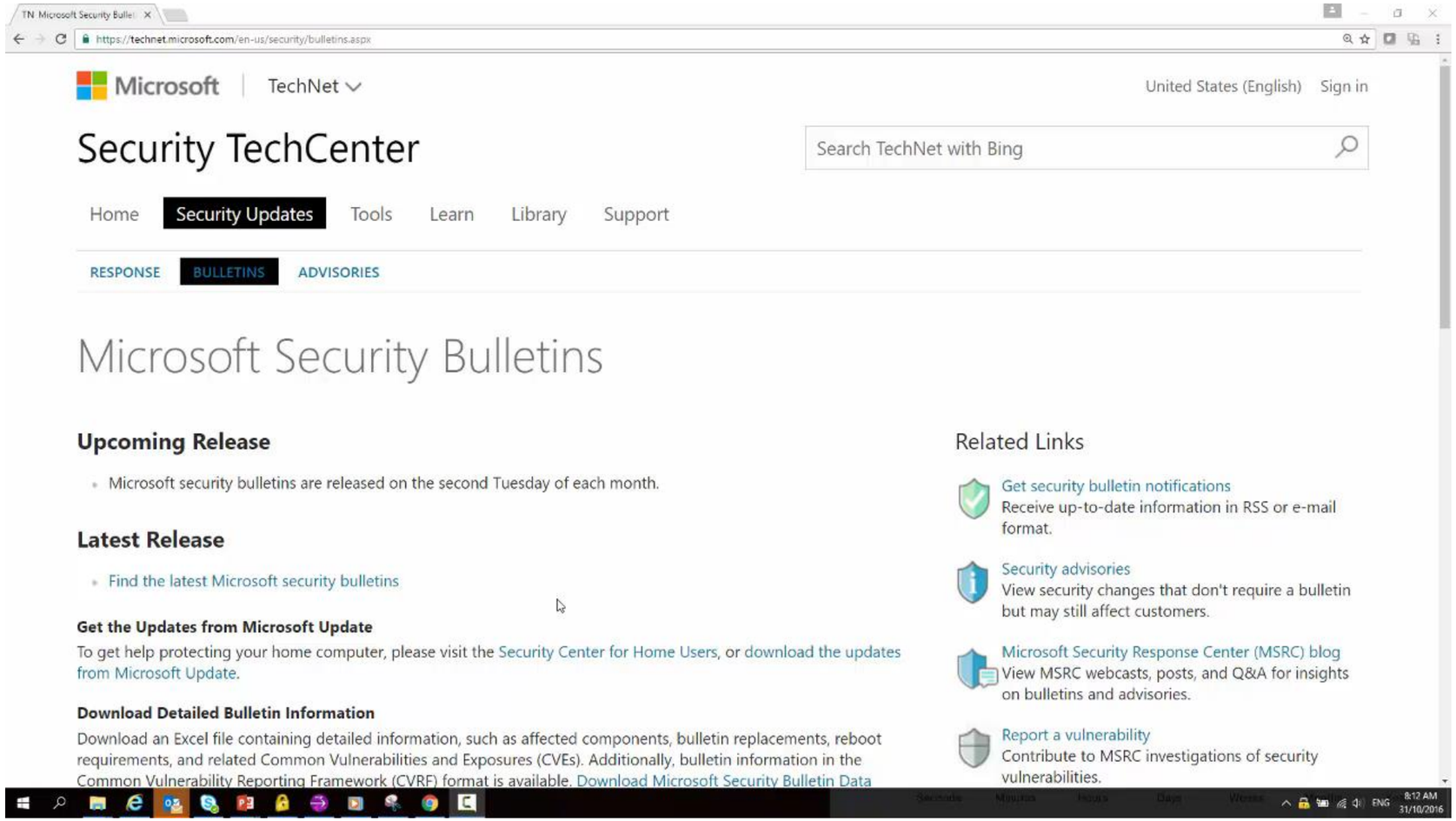
- **The EXPLOIT of a technical vulnerability**
- **Human error (still a vulnerability)**
- **Can involve chaining together a series of weaknesses**
- **Performed without owner permission**



What is Penetration Testing?

- **Similar to hacking except owner gives permission**
- **Attempt to gain access to sensitive information or resources**
- **Steps can include:**
  - Information gathering
  - Vulnerability enumeration
  - Vulnerability exploitation / Privilege Escalation
  - Exploration / Lateral Movements
- **Performed against defined scope**
- **Measures Network(s) and Application(s) resiliency**
- **Overall goal to improve security posture**

Almost ALWAYS Starts with a Vulnerability



Defining the “zero-day” (software) threat

A security hole in software that is **not yet known** to the software maker or to Information Security vendors	Code that attackers use to take **advantage** of a zero-day vulnerability to compromise a system for their benefit
NO PATCH – NO SIGNATURE	DROP - CONTROL - DISABLE
Zero-day vulnerability	Zero-day exploit

The term “zero-day” refers to the number of days that the software vendor has known about the hole - **ZERO**.

erabilities

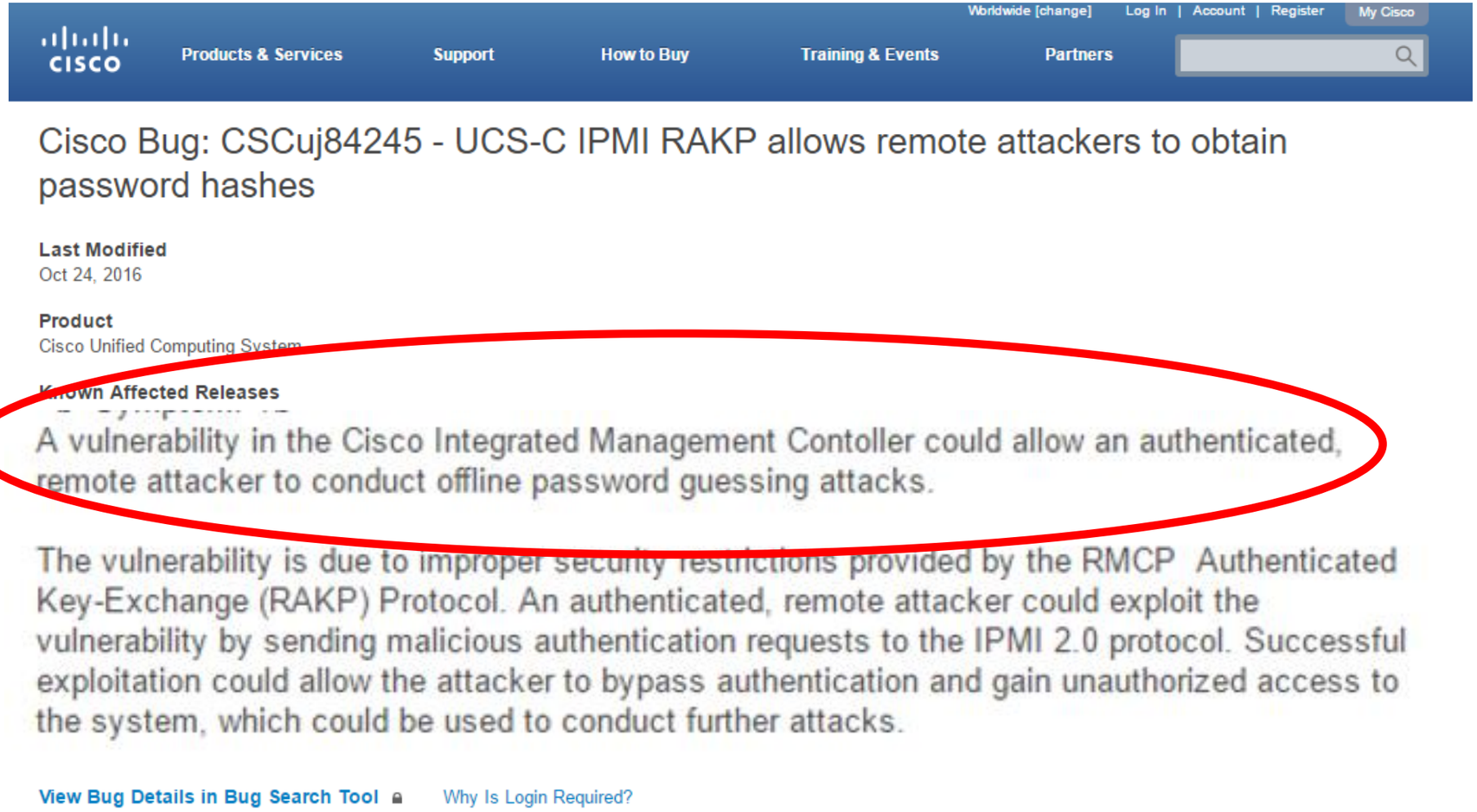
Google Discloses Windows Zero-Day Vulnerability

ovacs on November 01, 2016

59 G+1 9 Tweet Recommend 24 RSS

Google has disclosed a Windows zero-day vulnerability after Microsoft failed to release a patch within the 7-day deadline the search giant gives vendors when it finds a flaw that is actively exploited by malicious actors.

Example 1: Penetration Test



Worldwide [change] Log In | Account | Register My Cisco

Products & Services Support How to Buy Training & Events Partners

Cisco Bug: CSCuj84245 - UCS-C IPMI RAKP allows remote attackers to obtain password hashes

Last Modified
Oct 24, 2016

Product
Cisco Unified Computing System

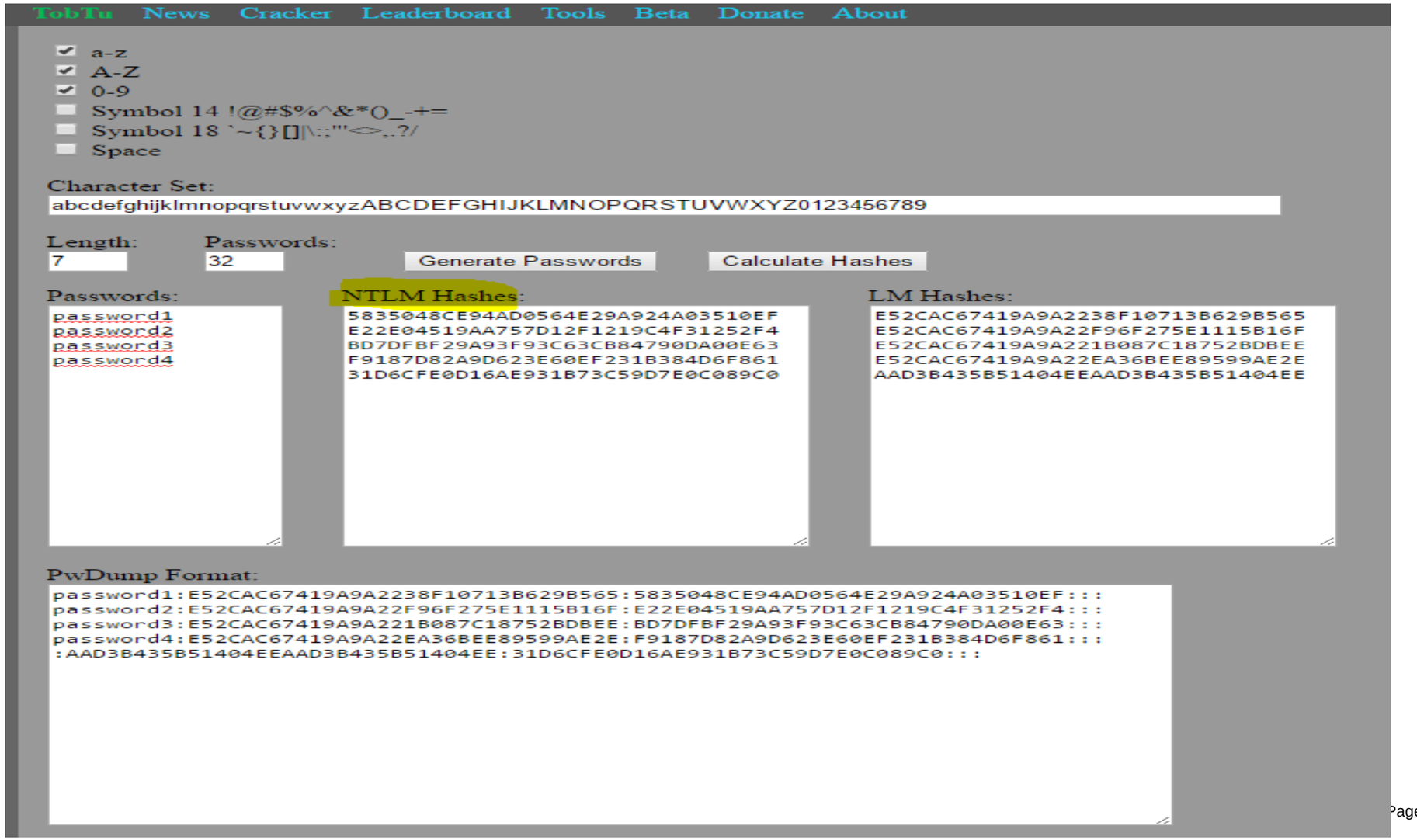
Known Affected Releases

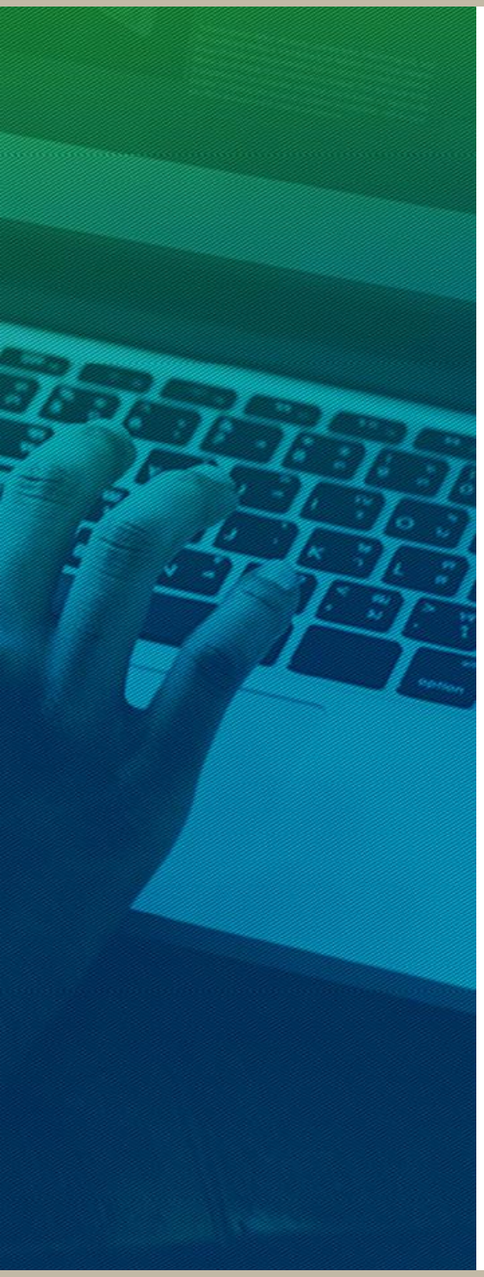
A vulnerability in the Cisco Integrated Management Contoller could allow an authenticated, remote attacker to conduct offline password guessing attacks.

The vulnerability is due to improper security restrictions provided by the RMCP Authenticated Key-Exchange (RAKP) Protocol. An authenticated, remote attacker could exploit the vulnerability by sending malicious authentication requests to the IPMI 2.0 protocol. Successful exploitation could allow the attacker to bypass authentication and gain unauthorized access to the system, which could be used to conduct further attacks.

View Bug Details in Bug Search Tool Why Is Login Required?

What Can You Do with Hash?





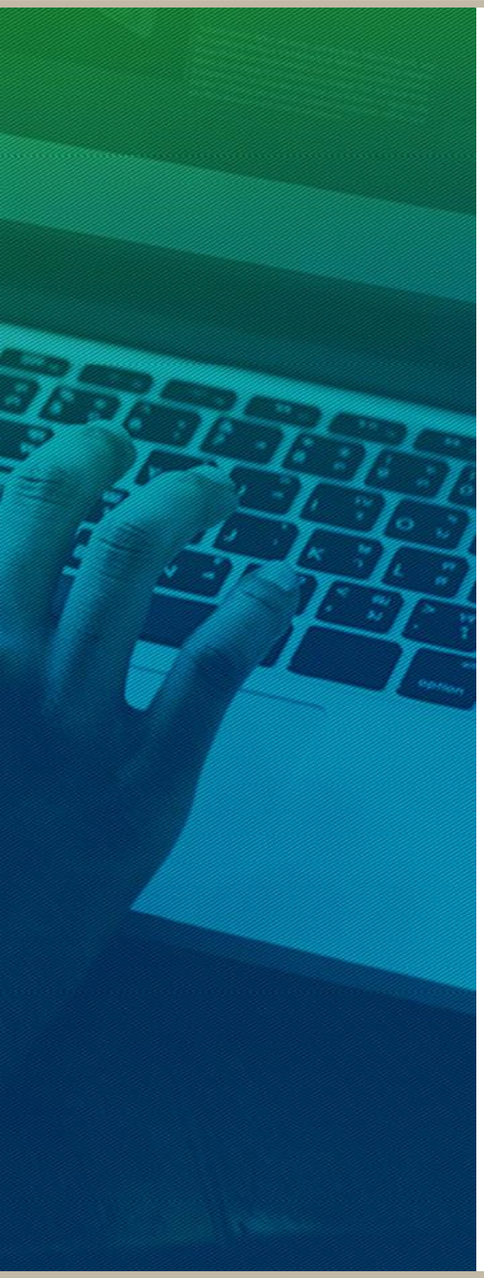
“Hashinator”

26 lower case letters (a-z)
26 upper case letters (A-Z)
10 digits (0-9)
8 Characters

26+26+10 = 62

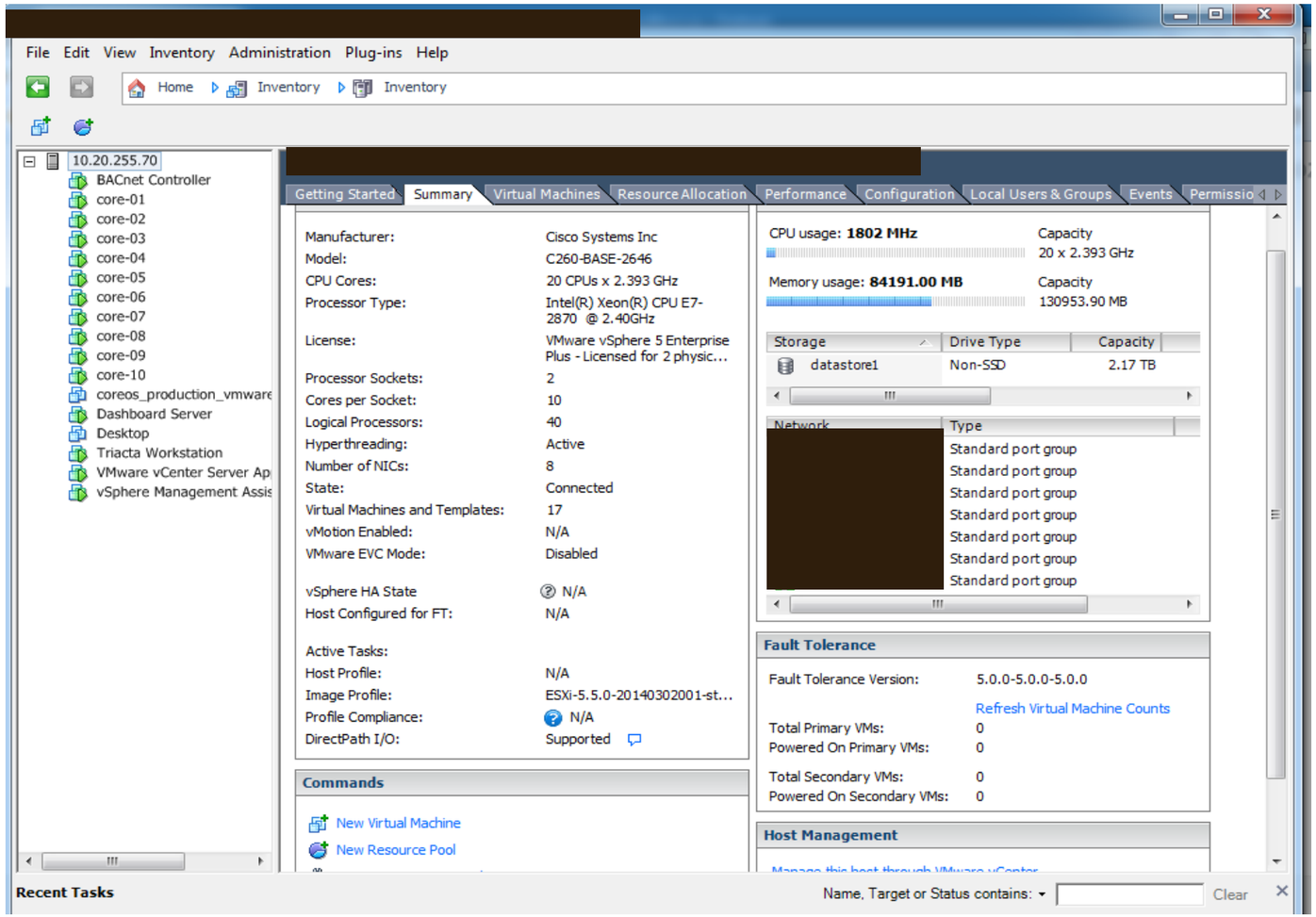
62 ^ 8 =
218,340,105,584,896

…or < 2 days

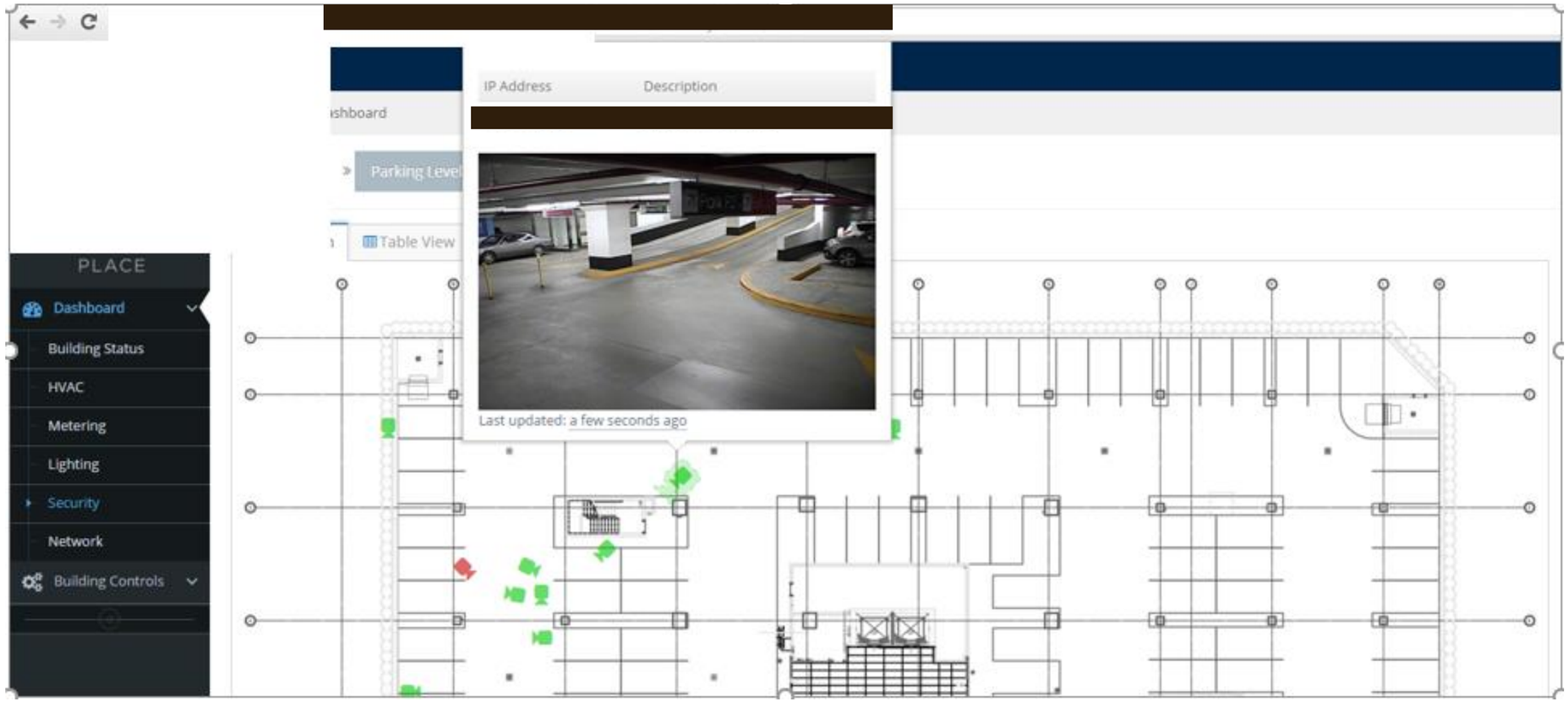


```
INFO: approaching final keyspace, workload adjusted

f7a0df1801200002f63d0c38641adeaee22884a29096a179270c2b069e96b48fa8314f2a1927111e
8db2de615edd11e3b960a80c0db8b7ec140561646d696e:0686e03152b9cef46e48fc82e94279cb0
6eec7ab:w [redacted] rk

Session.Name...: oclHashcat
Status.........: Cracked
Rules.Type.....: Generated (90000)
Input.Mode.....: File (/root/projects/[redacted]/working.txt)
Hash.Target....: f7a0df1801200002f63d0c38641adeaee22884a29...
Hash.Type......: IPMI2 RAKP HMAC-SHA1
Time.Started...: Mon Jan  4 18:51:01 2016 (2 secs)
Speed.GPU.#1...:  5054.6 kH/s
Speed.GPU.#2...:  5233.3 kH/s
Speed.GPU.#3...:  5281.1 kH/s
Speed.GPU.#4...:  5252.1 kH/s
Speed.GPU.#5...:  5239.2 kH/s
Speed.GPU.#*...: 26060.2 kH/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 52308480/110880000 (47.18%)
Rejected.......: 0/52308480 (0.00%)
Restore.Point..: 0/1232 (0.00%)
HWMon.GPU.#1...: 35% Util, 39c Temp, 20% Fan
HWMon.GPU.#2...: 61% Util, 34c Temp, 30% Fan
HWMon.GPU.#3...: 59% Util, 42c Temp, 30% Fan
HWMon.GPU.#4...: 61% Util, 37c Temp, 30% Fan
HWMon.GPU.#5...: 36% Util, 43c Temp, 20% Fan
```

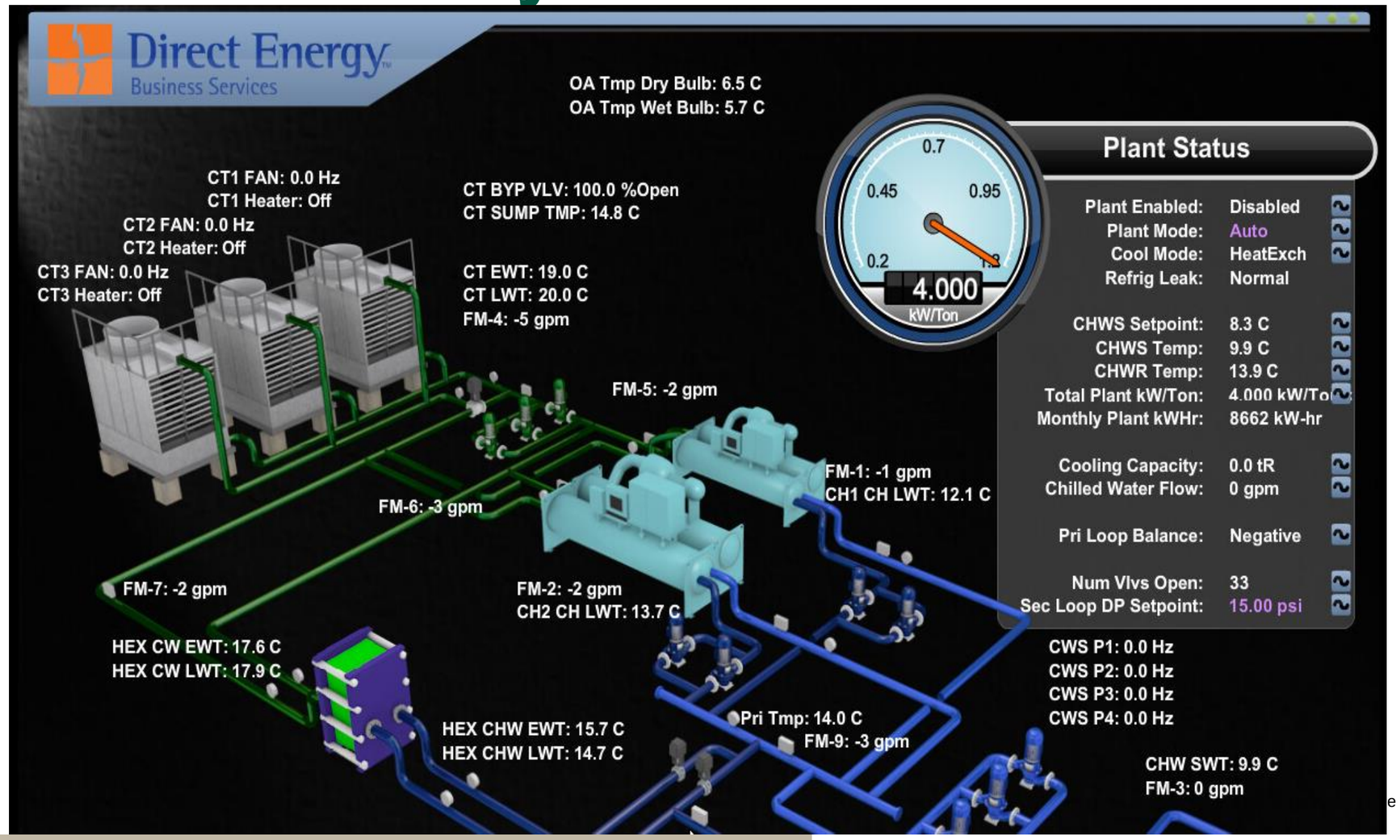
U/P Leads to Full VM Infrastructure



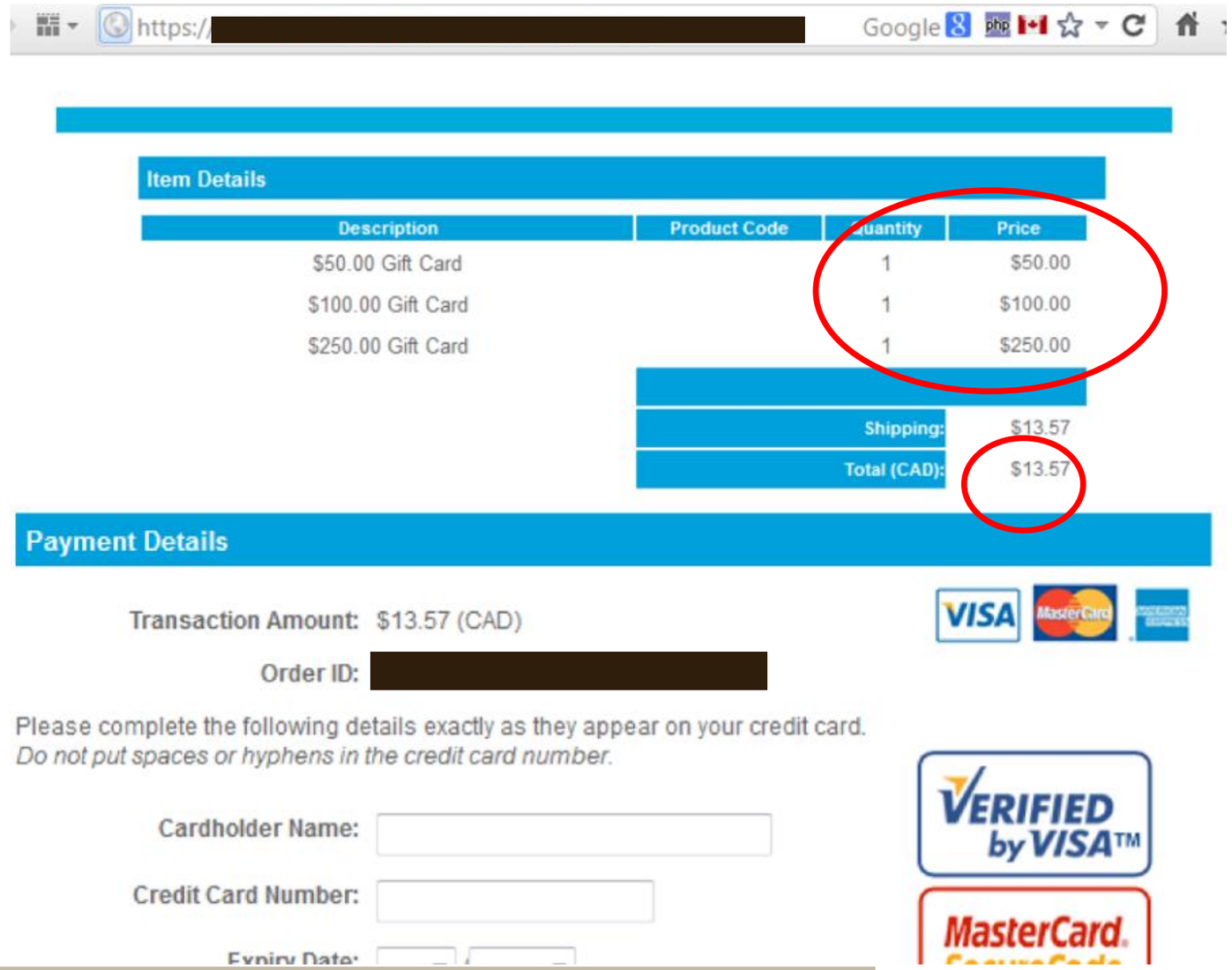
Once Access is Gained… Then We “Pivot”

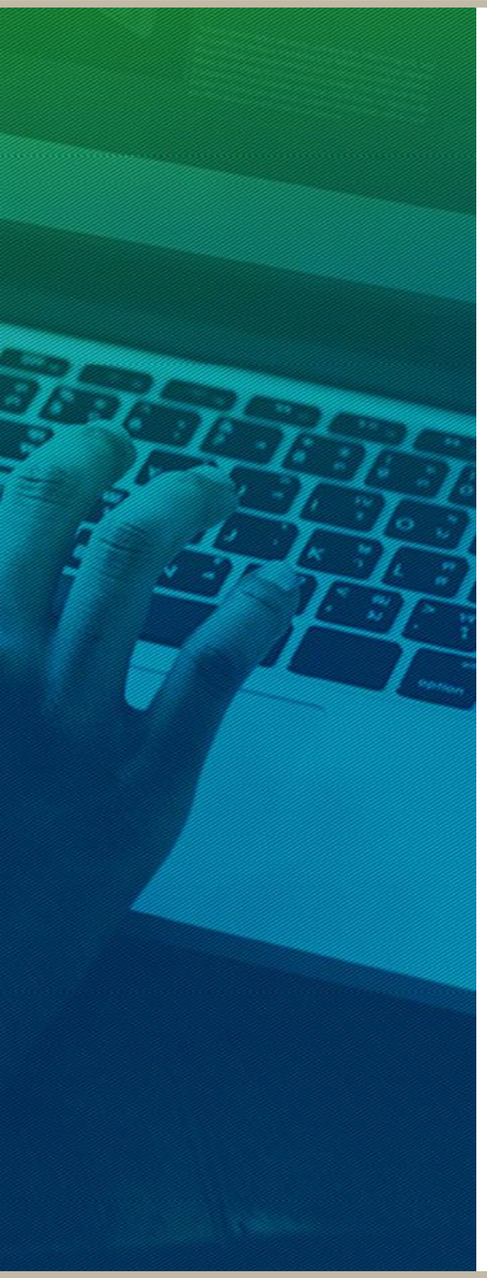


Access to HVAC System…



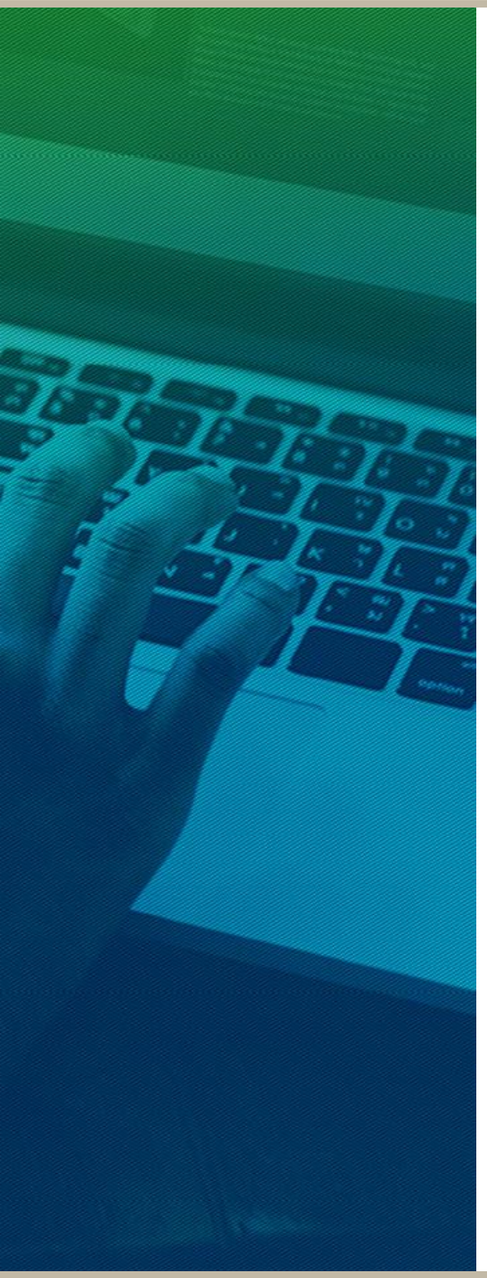
Example 2: Programming Error





What is Social Engineering?

- **An act that influences a person to take an action**
- **Used by attackers as it consistently works**
- **There is no patch for untrained users**
- **Performed against defined scope**
- **Three types of Social Engineering:**
  - Phishing
  - Vishing
  - Impersonation
- **Measures how well People identify SE attacks**



Example Phishing

Survey Monkey <survey@monkey.ca>

Mandatory employee survey

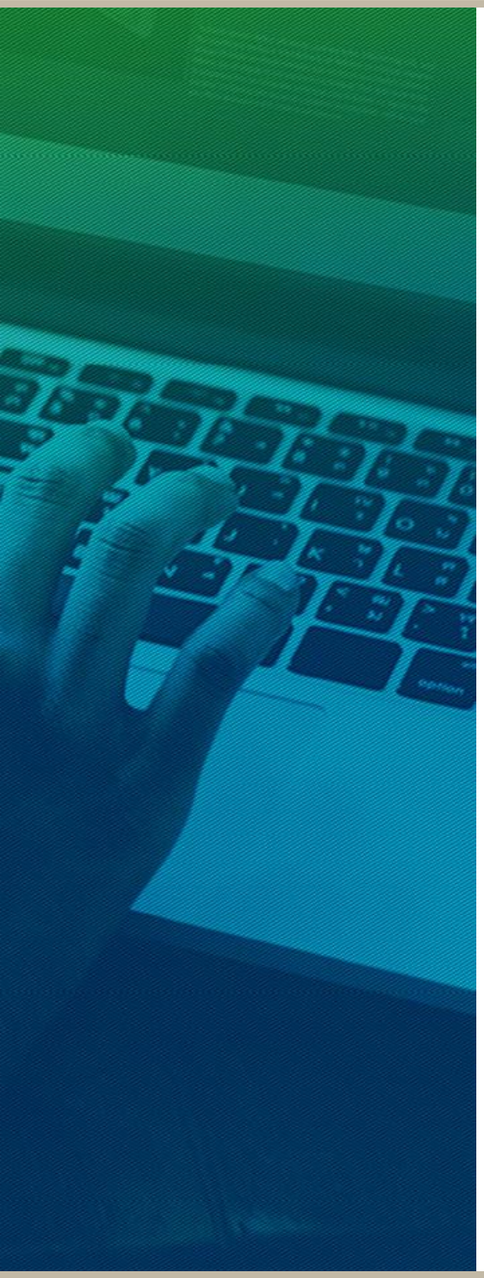
To

Hi,

This is a mandatory employee survey. Please fill out the following:

Survey

Thanks!



Mon 26/06/2017 11:42 AM

Linkedin Updates <messages-noreply@portal-linkedin.com>

Linkedin Updates

To

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

LinkedIn

[redacted] would like to connect on LinkedIn. How would you like to respond?

[redacted]

Associate Director, IT, ITIL, [redacted]
Corporation

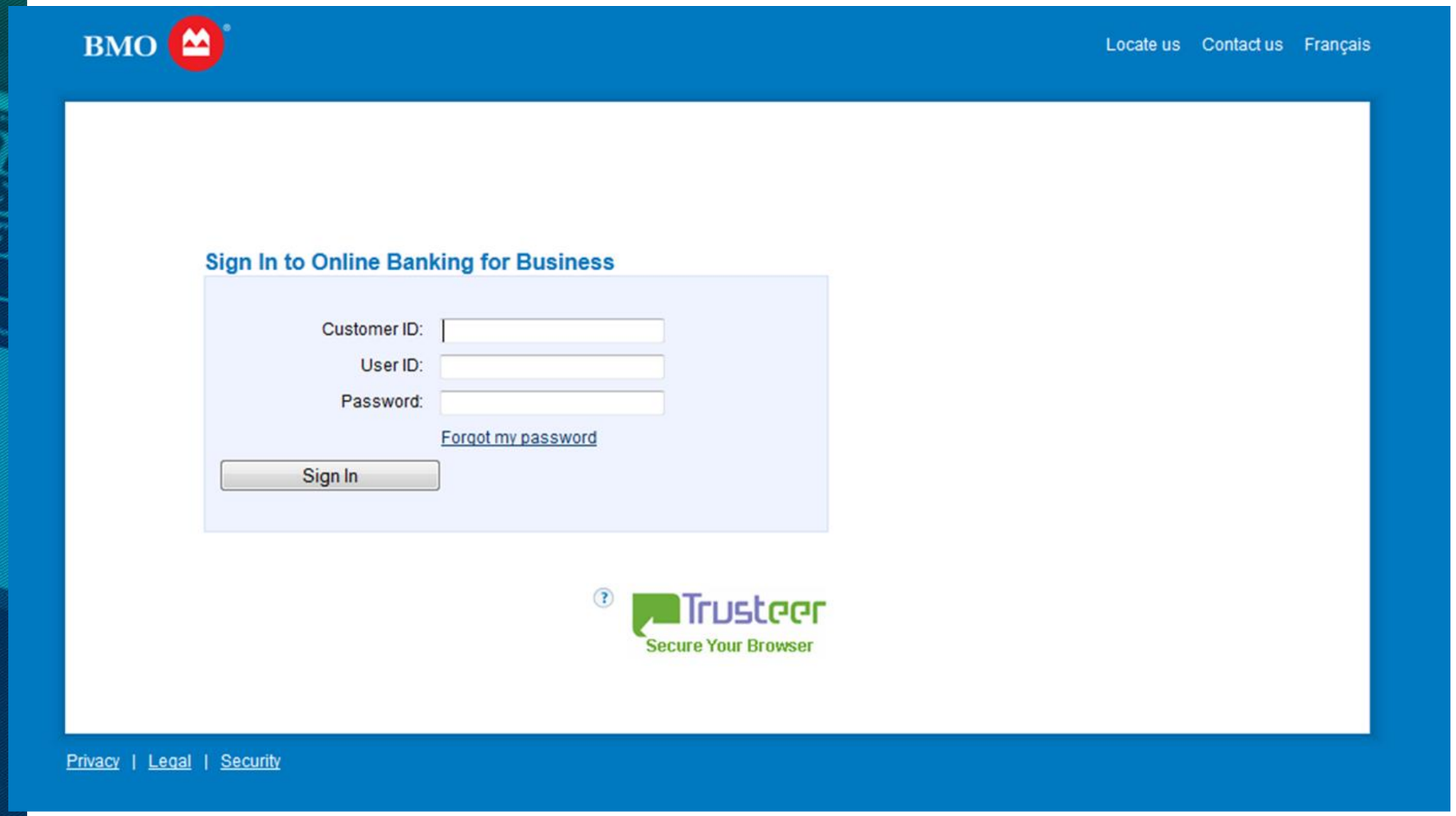
Confirm you know [redacted]

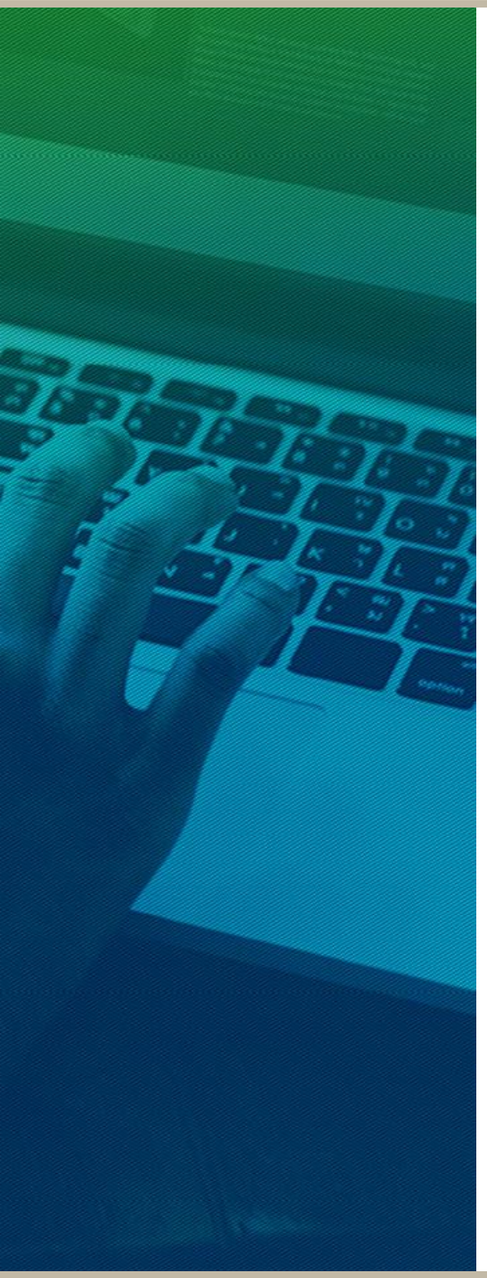
You are receiving Reminder emails for pending invitations. Unsubscribe

2017, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

Figure 2: Email 'being forwarded' to the recipients

Example 1: Phishing





Use the hover technique

Never click on URL's sent in emails…if you must, make sure you "hover" over the URL to see the REAL destination

Hi Everyone,

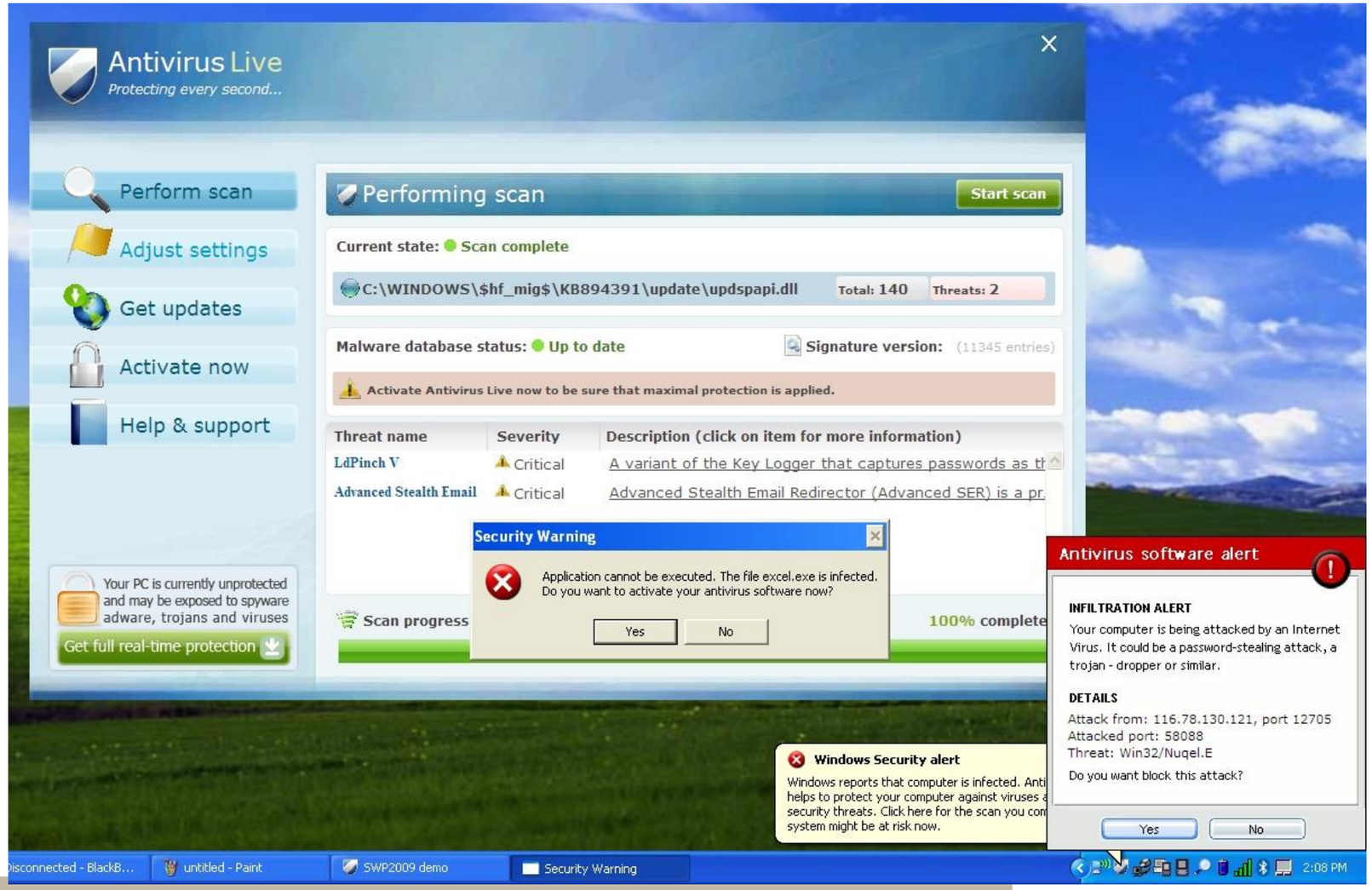
Due to the recent weather events in the Miami are
numbers on whether or not you will be attending t
located on The
https://theloop-mnp.ca/default.php?uid=lmnofhbx
Click or tap to follow link.
ease clic

http://agm.mnp.ca

The AGM website is accessible to partners only and
attendance.

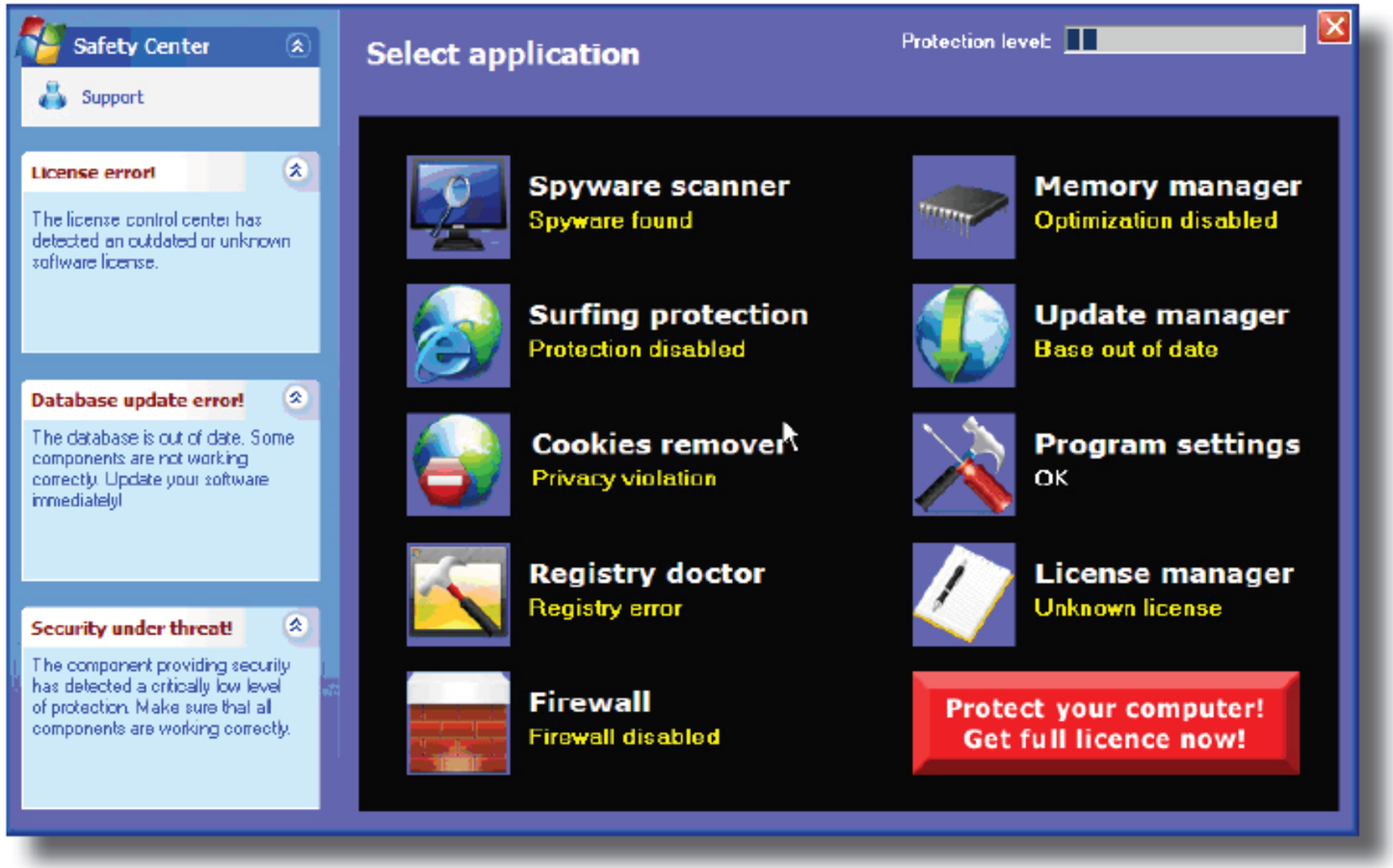
Hello, my name is XXXXX. Resume attached. I look forward to seeing you. Sincerely yours, XXXXX

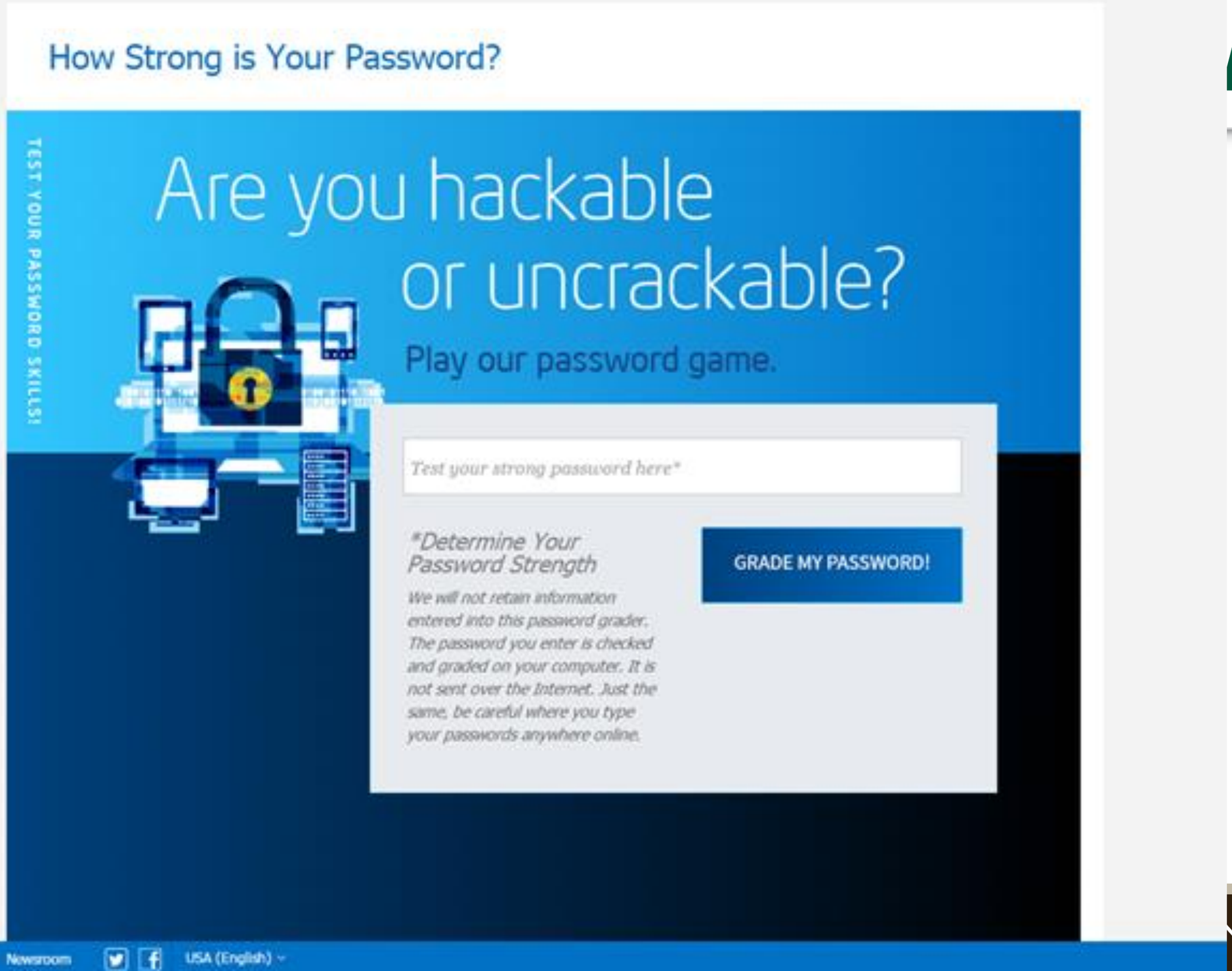
Example 5: Fake AV / Cryptolocker

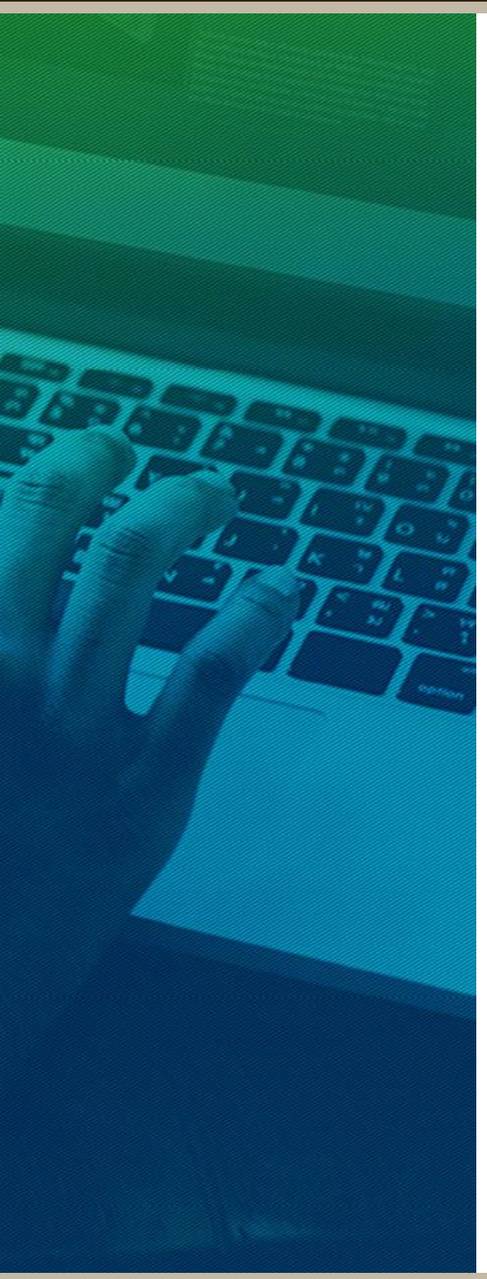


The following are some of the FAKEAV programs that the KOOBFACE botnet pushes:

- ***Safety Center.*** This offers two types of license:
  - **One-year license:** This is worth US$59.95.
  - **Lifetime license:** This is worth US$79.95.




How Strong is Your Password?
TEST YOUR PASSWORD SKILLS!
Are you hackable
or uncrackable?
Play our password game.
Test your strong password here*
*Determine Your Password Strength
We will not retain information entered into this password grader. The password you enter is checked and graded on your computer. It is not sent over the Internet. Just the same, be careful where you type your passwords anywhere online.
GRADE MY PASSWORD!
Newsroom
USA (English)



Executive Wire Fraud

- **Social Engineering w/o Malware**

5 Votes

Scammers pose as company execs in wire transfer spam campaign

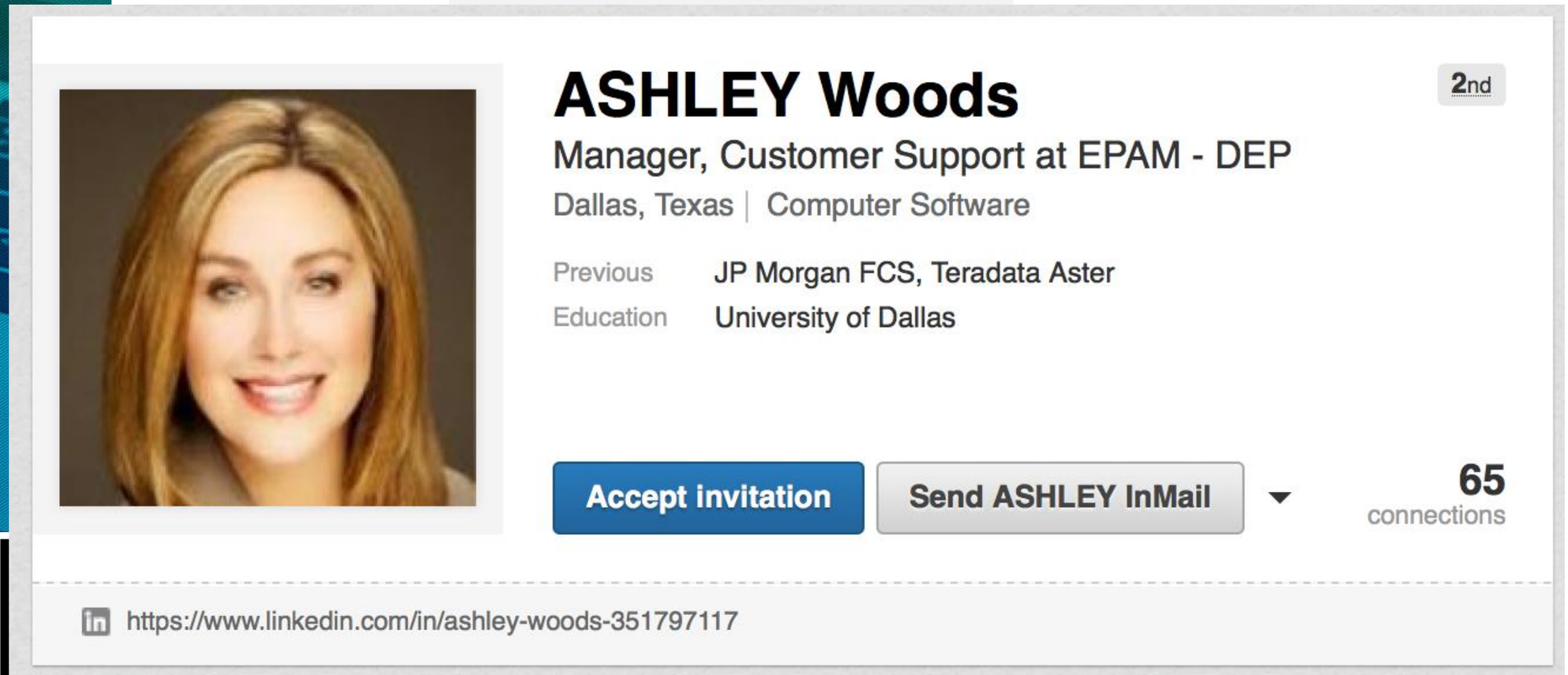
Innocent-looking payment requests could result in financial loss for companies as finance department employees targeted with fraudulent emails.

By: **Sean Butler** SYMANTEC EMPLOYEE

Created 28 Oct 2014

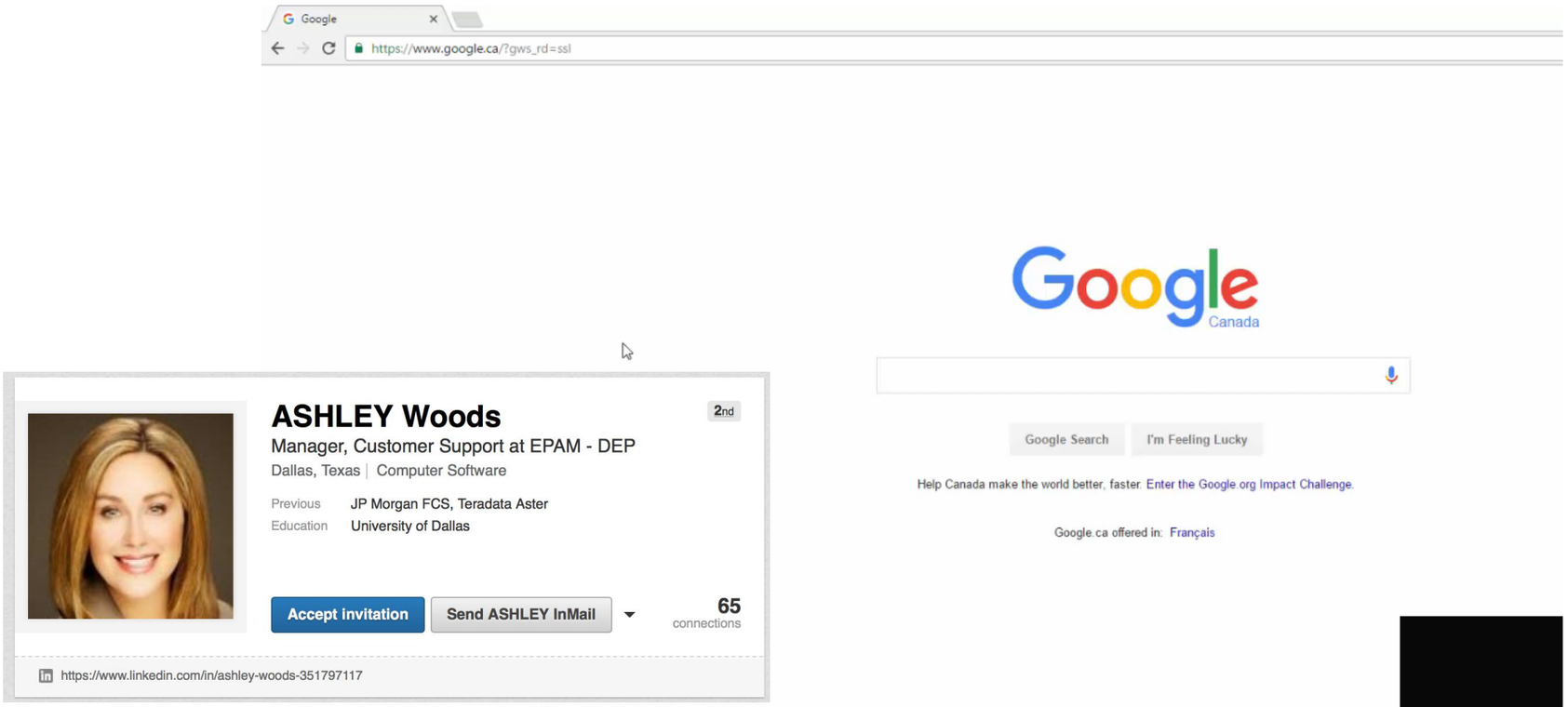
0 Comments | Translations: Português | Share

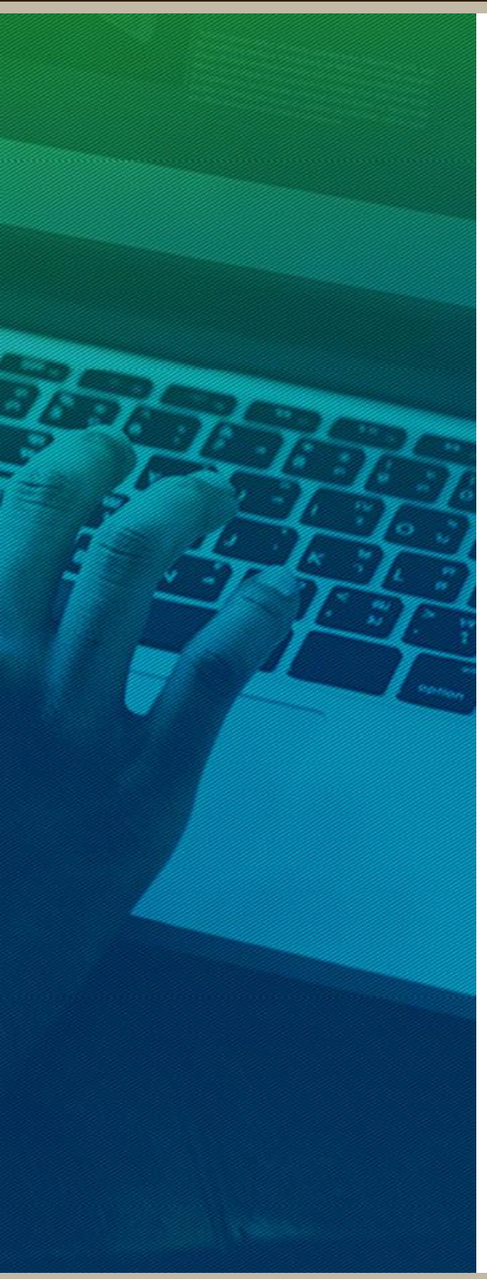
Social Engineering Attackers Deploy Fake Social Media Profiles



Tip #3 – Google Images

- Use Google Images to verify and validate pictures



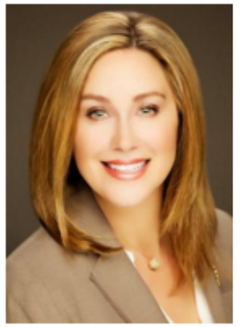


NBC AFFILIATES | REPORTING | SHOPTALK

Reporter Deborah Sherman Out At Denver's KUSA

Share Tweet More

By Merrill Knox on Nov. 22, 2011 - 12:35 PM 1 Comment

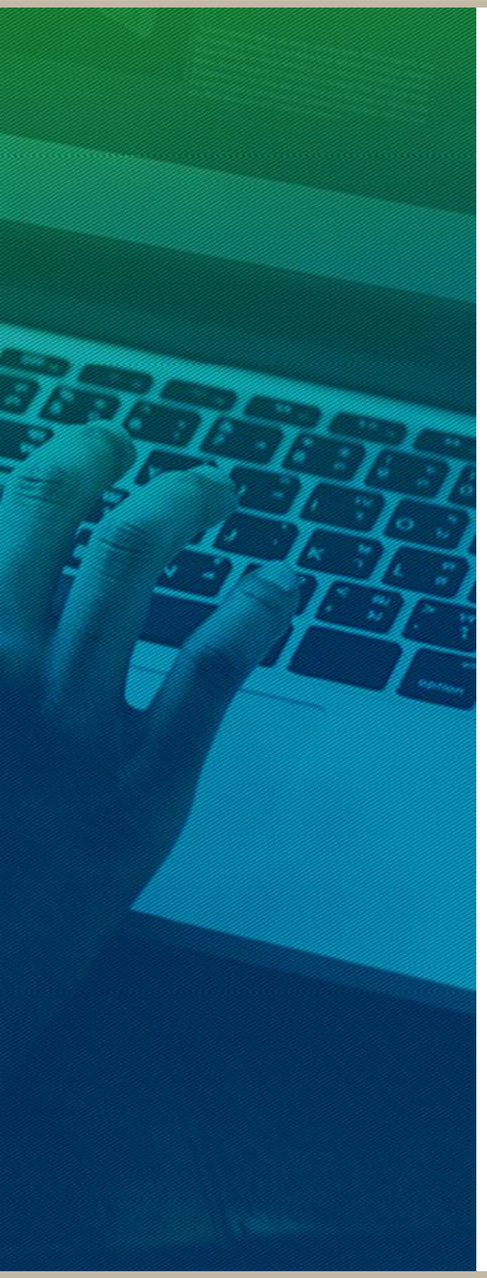


Deborah Sherman, a reporter at KUSA, has been cut loose at the Denver NBC-affiliate because of a "personnel issue," the *Denver Post* reports.

Sherman joined KUSA's investigative reporting team in 2003. Her last day at the station was reportedly last week, though management has refused comment on the circumstances surrounding her departure.

"We're not going to comment on people who are leaving or have left the station," KUSA news director Patti Dennis said.

The *Post* reports Sherman "is said to have great contacts but not the easiest professional temperament," saying a memo from station management to KUSA staffers fueled rumors that Sherman was shown the door due to her connection to several controversial stories she has reported on in the past.



What is Red Teaming?

- **Contains aspects of Penetration Testing and Social Engineering**
- **Performed with the permission of the owner**
- **Typically full-scope, multi-layered attack simulation**
  - Penetration Testing
  - Social Engineering
  - Physical Security Controls
- **Designed to measure resiliency of People, Network(s), and Application(s) during a real-life attack**
- **Attacks are performed simultaneously**
- **Overall goal to identify gaps and improve Incident Response**

Considerations

Top 10 Considerations

Have you and your executives quantified business risk? What is the impact to those assets if breached? How to better prioritize budget & resources?

Have you developed and implemented the appropriate cyber security infrastructure to protect your organization and maintain your clients' confidence?

Have you understood your potential exposure by engaging cyber security consultants "ethical hackers" to hack your organization? (Networks, Applications, Mobile)

Top 10 Considerations

Can you demonstrate a solid Cyber Incidence Response plan which enables you to respond to a breach? If yes, have you tested it by doing a table top exercise?

Have you ever considered a Cyber Security Advisor (Virtual Chief Information Security Officer-VCISO) to help set standards and policies?

Do you have a clear understanding of your Supply Chain/Vendor/Third Party Management Strategy & Contracts; beginning with the IT focused contracts?

Top 10 Considerations

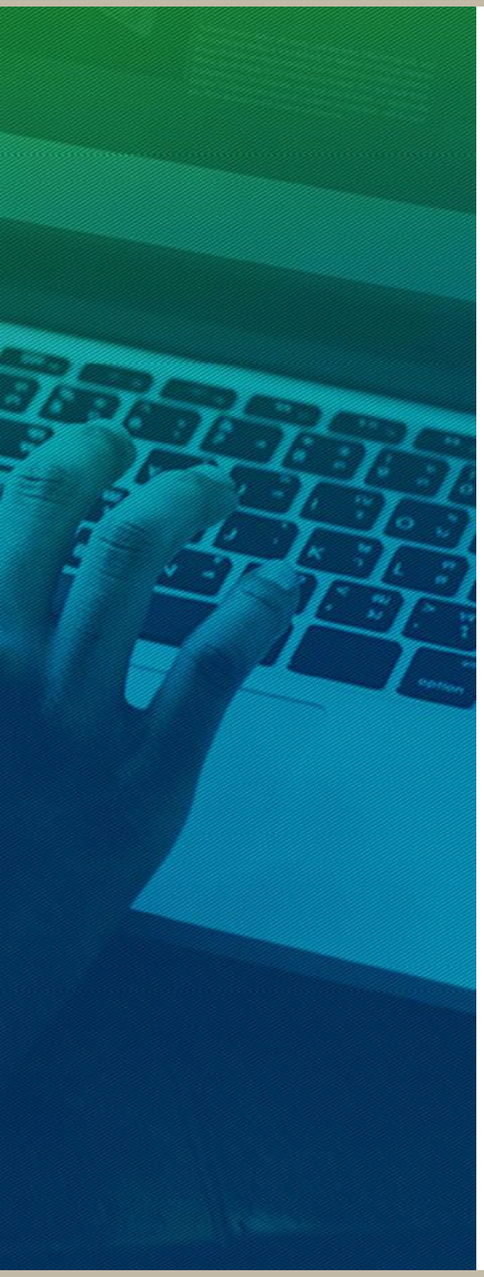
Have you considered purchasing cyber security-specific insurance to protect against the ramifications of any major breaches? Is it focused on the key business risks identified if breached?

Is your information reinforced by a business continuity plan including data backup & data recovery. Is the data stored offline & offsite? Have you tried restoring it?

Top 10 Considerations

How sophisticated are your Cyber Security Educational Training, practices and procedures? Are you making it personal?

Do you have a patching and shadow IT strategy? Two of the biggest problems that exist in Cyber Security today.



Cyber Security Services

Offensive Security (Red Team)

- Penetration Testing
- Blended Threat Attack Exercises
- Social Engineering
- Vulnerability Assessments

Defensive Security (Blue Team)

- Enterprise Network Security
- Network, Wireless and Security Architectural Design
- Perimeter and Data Center Security
- Data Loss Prevention and Data Encryption
- Email / Web Content Filtering and Malware Protection
- Secure Access and Authentication
- End Point Security and Encryption
- Wireless, BYOD and Network Access Control
- Security Hardening Standards and Guidelines
- Virtualization and Cloud Computing Standards and Guidance
- Security Awareness Training

Forensics

- Data Retrieval from hard drives, servers, laptops, cell phones, etc.
- E-Discovery Service for Court Admissibility

Risk Management

- Quantitative Threat and Risk Assessment (based on probabilities and industry statistics
- Qualitative Threat and Risk Assessment (based on matrix approach)
- Cloud Security Checklist
- Privacy Impact Assessments
- MTA (Maturity Threat Analysis)
- Information Security Framework Development
- Assessment and Review against ISO27k, NIST, CSF or CSC 20
- Policy, Process, Procedure and Documentation Development

Payment Card Industry (PCI) Compliance

- Scope Discovery
- Gap Analysis and Readiness Review
- On Demand Consulting and Remediation
- PCI Report on Compliance Validation (ROC)
- PCI SAQ Review and Sign Off
- External ASV Scanning
- Annual Maintenance (Business as Usual)

Managed Services

- Cyber Security Administration
- Perimeter Threat Prevention (firewall, IPS, anti-virus, web application firewalls, etc.)
- 2-Factor Authentication
- Log Management

Questions?

Danny Timmins
National Leader Cyber Security

Danny.Timmins@MNP.CA