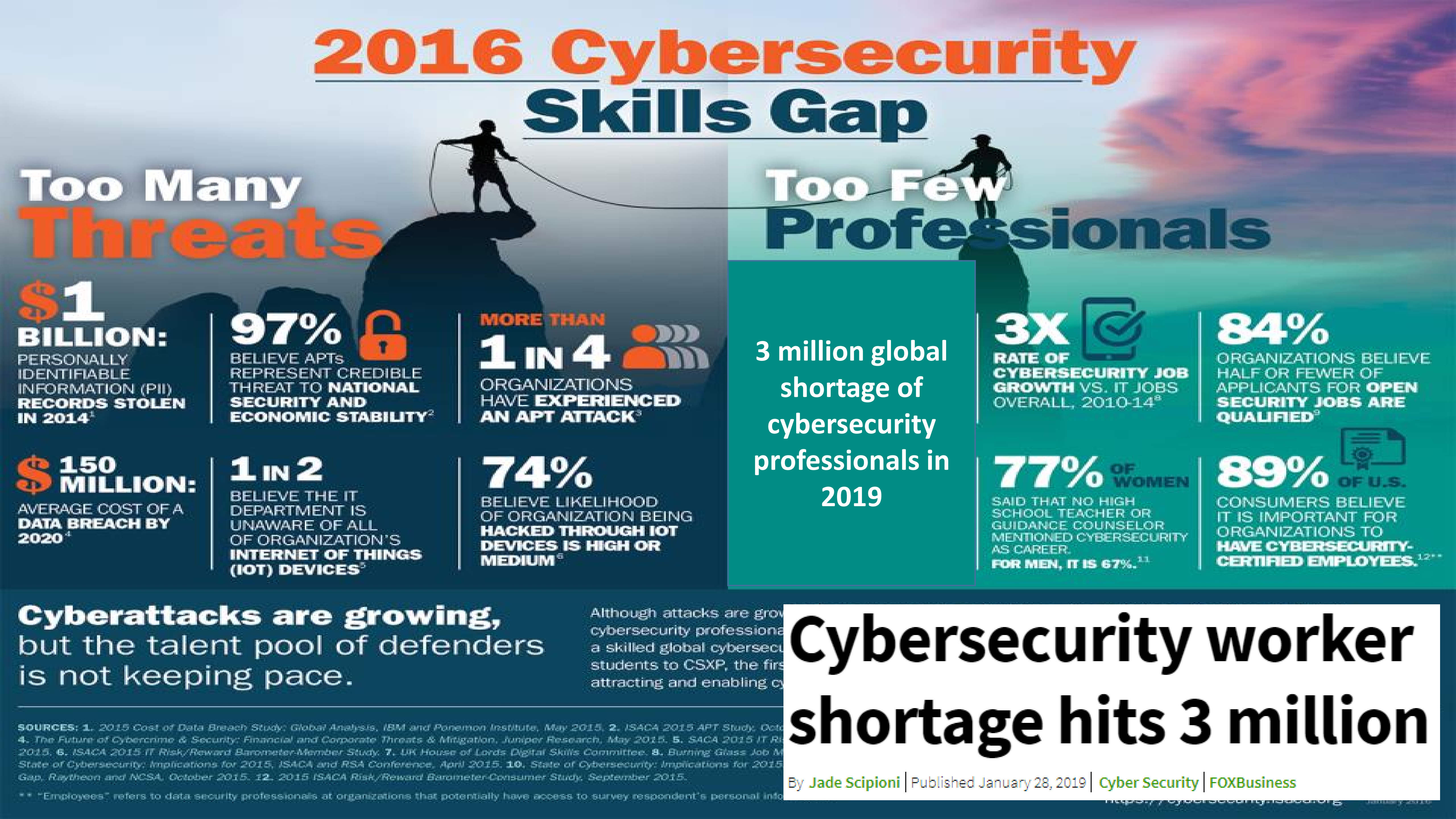
Humans of Security

November 2019

Gary Perkins, MBA, CISSP
Chief Information Security Officer (CISO)
Executive Director, Information Security Branch



2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN **1 IN 4** ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

3 million global shortage of cybersecurity professionals in 2019

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are grow
cybersecurity professiona
a skilled global cybersecu
students to CSXP, the firs
attracting and enabling cy

Cybersecurity worker shortage hits 3 million

By Jade Scipioni | Published January 28, 2019 | Cyber Security | FOXBusiness

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, Octo*
4. *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *SACA 2015 IT Ri*
2015. **6.** *ISACA 2015 IT Risk/Reward Barometer-Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job M*
State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. **10.** *State of Cybersecurity: Implications for 2015*
Gap, Raytheon and NCSA, October 2015. **12.** *2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.*

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal info

https://cybersecurity.isaca.org

January 2016

Talent Shortage

0%

cybersecurity

unemployment in BC

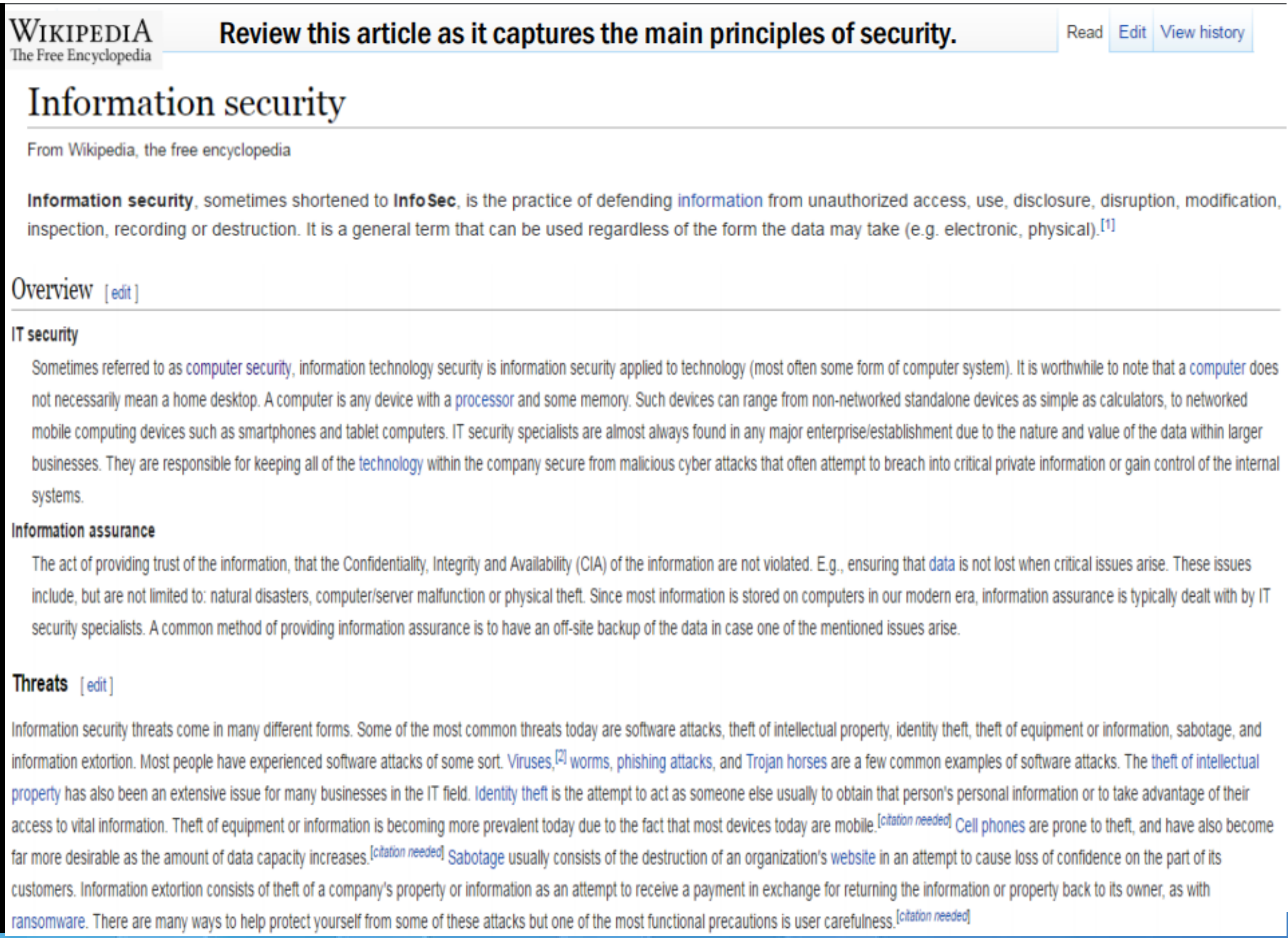
Career in Security

https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/information-security-awareness/careers_in_cybersecurity.pdf

https://en.wikipedia.org/wiki/Information_security

Security career

1



Review this article as it captures the main principles of security.

Information security

From Wikipedia, the free encyclopedia

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).[1]

Overview [edit]

IT security

Sometimes referred to as computer security, information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance

The act of providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated. E.g., ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

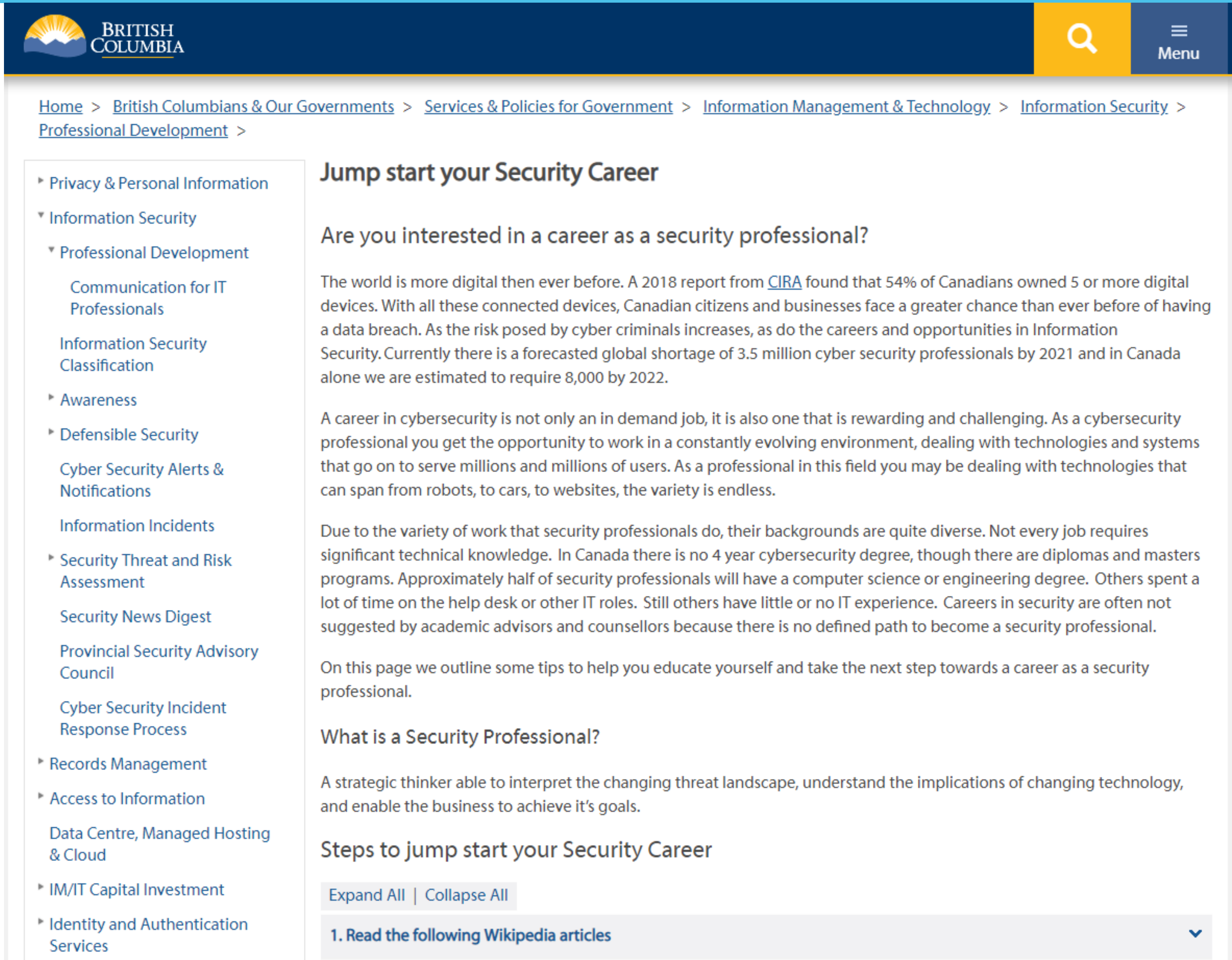
Threats [edit]

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses,[2] worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile.[citation needed] Cell phones are prone to theft, and have also become far more desirable as the amount of data capacity increases.[citation needed] Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.[citation needed]

Career in Security

Visit our webpage and jumpstart your security career…

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/professional-development/jump-start-your-security-career


BRITISH COLUMBIA
Menu
Home > British Columbians & Our Governments > Services & Policies for Government > Information Management & Technology > Information Security > Professional Development >
Privacy & Personal Information
Information Security
Professional Development
Communication for IT Professionals
Information Security Classification
Awareness
Defensible Security
Cyber Security Alerts & Notifications
Information Incidents
Security Threat and Risk Assessment
Security News Digest
Provincial Security Advisory Council
Cyber Security Incident Response Process
Records Management
Access to Information
Data Centre, Managed Hosting & Cloud
IM/IT Capital Investment
Identity and Authentication Services
Expand All | Collapse All

Jump start your Security Career

Are you interested in a career as a security professional?

The world is more digital then ever before. A 2018 report from CIRA found that 54% of Canadians owned 5 or more digital devices. With all these connected devices, Canadian citizens and businesses face a greater chance than ever before of having a data breach. As the risk posed by cyber criminals increases, as do the careers and opportunities in Information Security. Currently there is a forecasted global shortage of 3.5 million cyber security professionals by 2021 and in Canada alone we are estimated to require 8,000 by 2022.

A career in cybersecurity is not only an in demand job, it is also one that is rewarding and challenging. As a cybersecurity professional you get the opportunity to work in a constantly evolving environment, dealing with technologies and systems that go on to serve millions and millions of users. As a professional in this field you may be dealing with technologies that can span from robots, to cars, to websites, the variety is endless.

Due to the variety of work that security professionals do, their backgrounds are quite diverse. Not every job requires significant technical knowledge. In Canada there is no 4 year cybersecurity degree, though there are diplomas and masters programs. Approximately half of security professionals will have a computer science or engineering degree. Others spent a lot of time on the help desk or other IT roles. Still others have little or no IT experience. Careers in security are often not suggested by academic advisors and counsellors because there is no defined path to become a security professional.

On this page we outline some tips to help you educate yourself and take the next step towards a career as a security professional.

What is a Security Professional?

A strategic thinker able to interpret the changing threat landscape, understand the implications of changing technology, and enable the business to achieve it's goals.

Steps to jump start your Security Career

1. Read the following Wikipedia articles

Cybersecurity has never been as imperative

Bell
ebay
tumblr.
TARGET
STAPLES
Marriott
Australian Government
YAHOO!
HOLLYWOOD PRESBYTERIAN MEDICAL CENTER
craigslist
SONY
Quora
JPMorganChase
T·J·maxx
UNIVERSITY OF CALGARY
UKRAINE
UNDER ARMOUR
accenture
Ontario
Adobe
Google
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
UBER
EQUIFAX
Canada
ASHLEY MADISON.com
BRITISH AIRWAYS
BANGLADESH BANK
Central Bank of Bangladesh
NRC·CNRC
CATHAY PACIFIC
ATLANTA
FORRESTER
Ottawa
living social
EVERNOTE
THE HOME DEPOT
aws
Deloitte.
Anthem

Recent Study

A study this year of the highest profile breaches revealed they could have been prevented with one or more of the following:

1) security awareness
2) patching
3) offline backups
4) password management
5) supply chain security

ABC’s of Security

Awareness

Backups

Patching

Humans of Security

motivation

Executives

- language

Threat Actors or Cybercriminals

- types
- sophistication
- resources

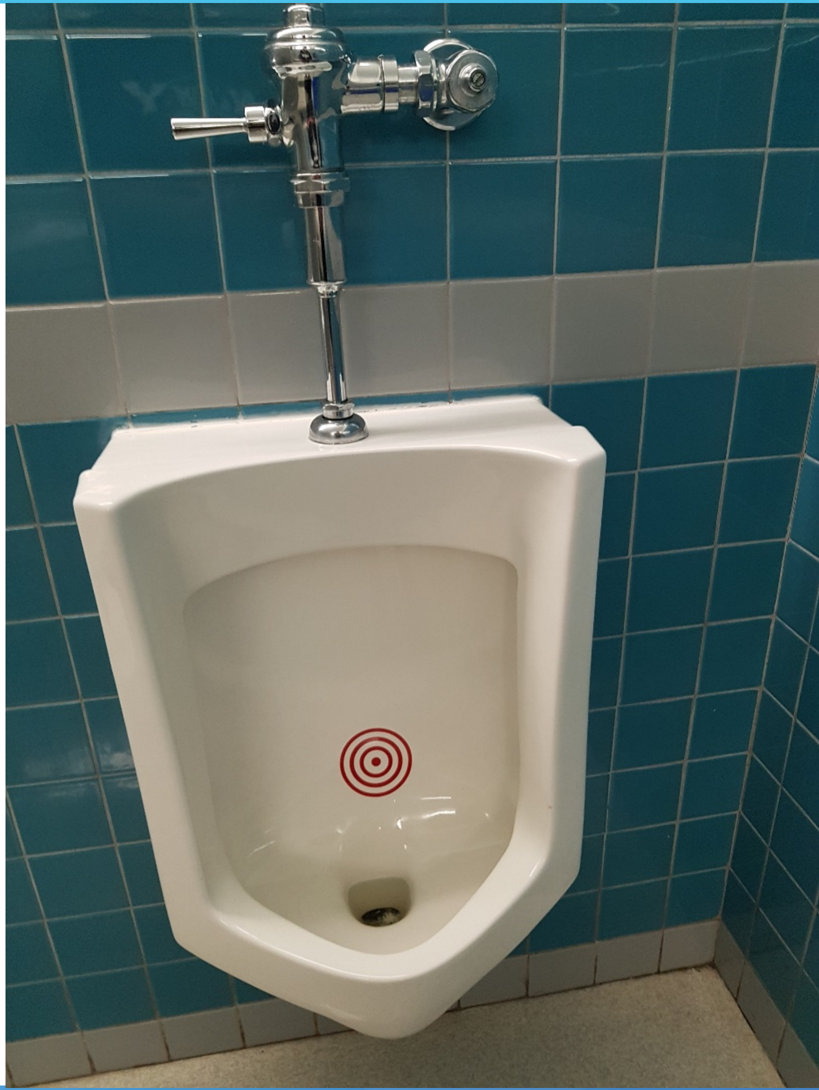
Employees

- weakest link or strongest asset?

Security Professionals

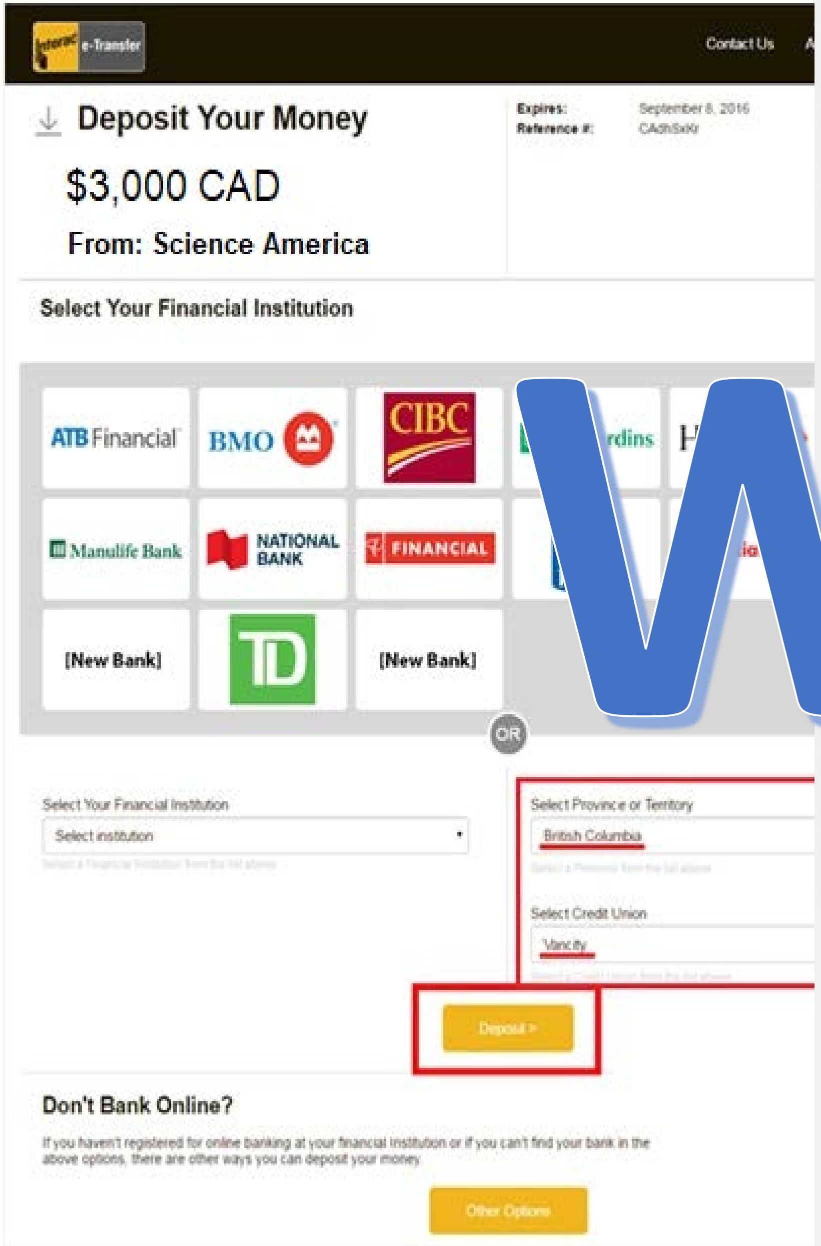
Nudge Theory

- concept in behavioral science, political theory and behavioral economics
- proposes positive reinforcement and indirect suggestions to influence behavior and decision making of groups or individuals
- can’t remove options, individual must be free to choose
- just incent them to choose the right option



Wikipedia

Example: Security Quest



Deposit Your Money

$3,000 CAD

From: Science America

Expires:	September 8, 2016
Reference #:	CAdhSxKr

Select Your Financial Institution

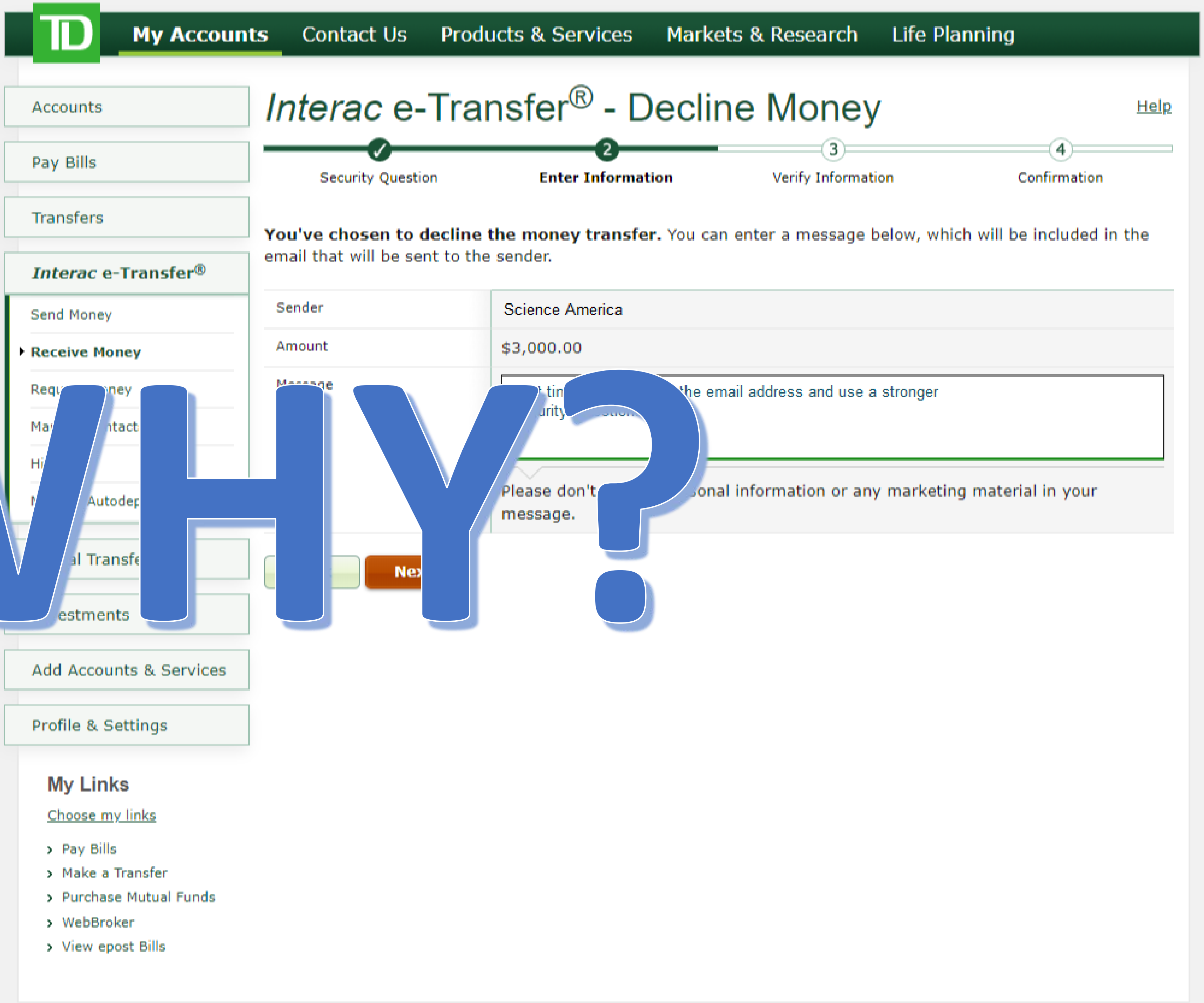
Select Your Financial Institution: Select institution

Select Province or Territory: British Columbia

Select Credit Union: Vancity

Don't Bank Online?

If you haven't registered for online banking at your financial institution or if you can't find your bank in the above options, there are other ways you can deposit your money



My Links

Choose my links

- Pay Bills
- Make a Transfer
- Purchase Mutual Funds
- WebBroker
- View epost Bills

Interac e-Transfer® - Decline Money

You've chosen to decline the money transfer. You can enter a message below, which will be included in the email that will be sent to the sender.

Sender	Science America
Amount	$3,000.00
Message	t tin the email address and use a stronger urity

Please don't onal information or any marketing material in your message.

WHY?

Example: Ransomware

Ransomware attack knocks Nunavut government services offline

Nunavut government rebuilding network after ransomware attack

All Word documents and PDF files the virus had access to are encrypted and unreadable by the government, according to Martin Joy, Nunavut's director of information, communications and technology.

According to their investigatio government's network around (IT) staff had confirmed the at

The virus was likely downloade Friday night clicked on a web a

Joy said security systems in pla looks like the DoppelPaymer, a systems weren't yet trained to detect, Joy said.

Canadian Nunavut government systems crippled by ransomware

ing computers for twork

ing again within a week or two

still locked out of kend

ransomware attack

Nunavu governn

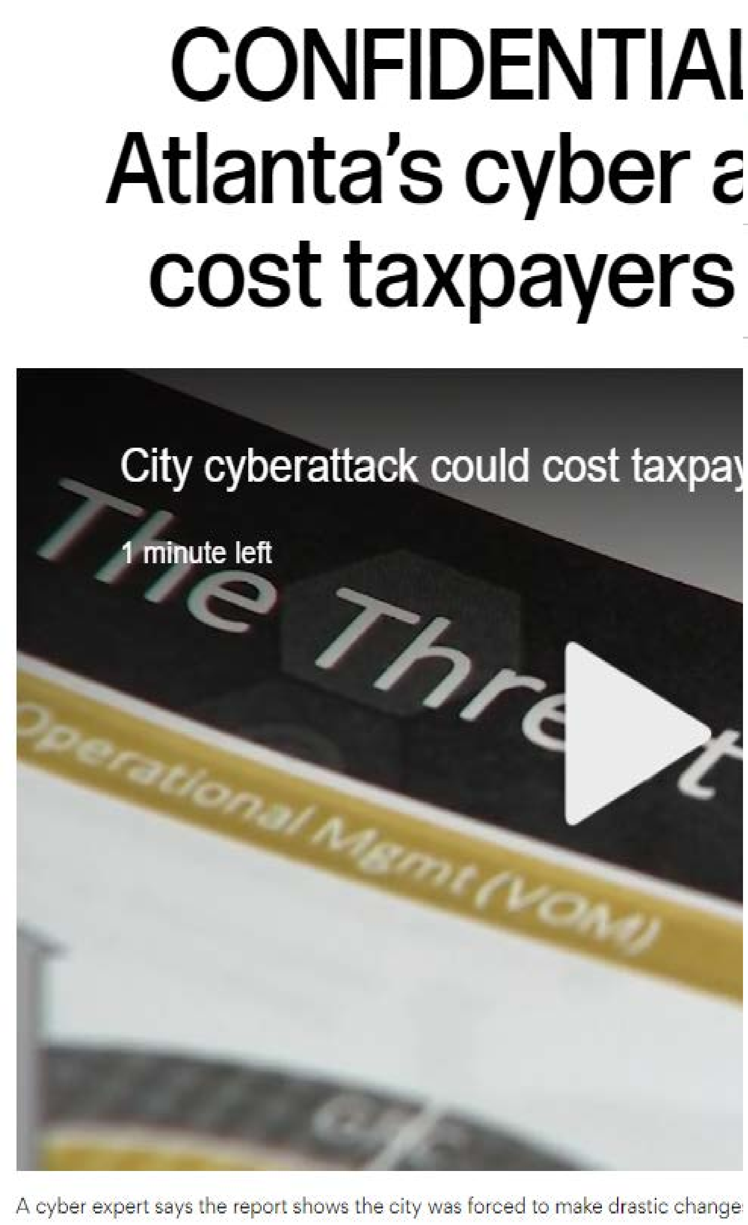
kend

Ransom government services offline

are attack

Backups

T is for "Tuition Value"

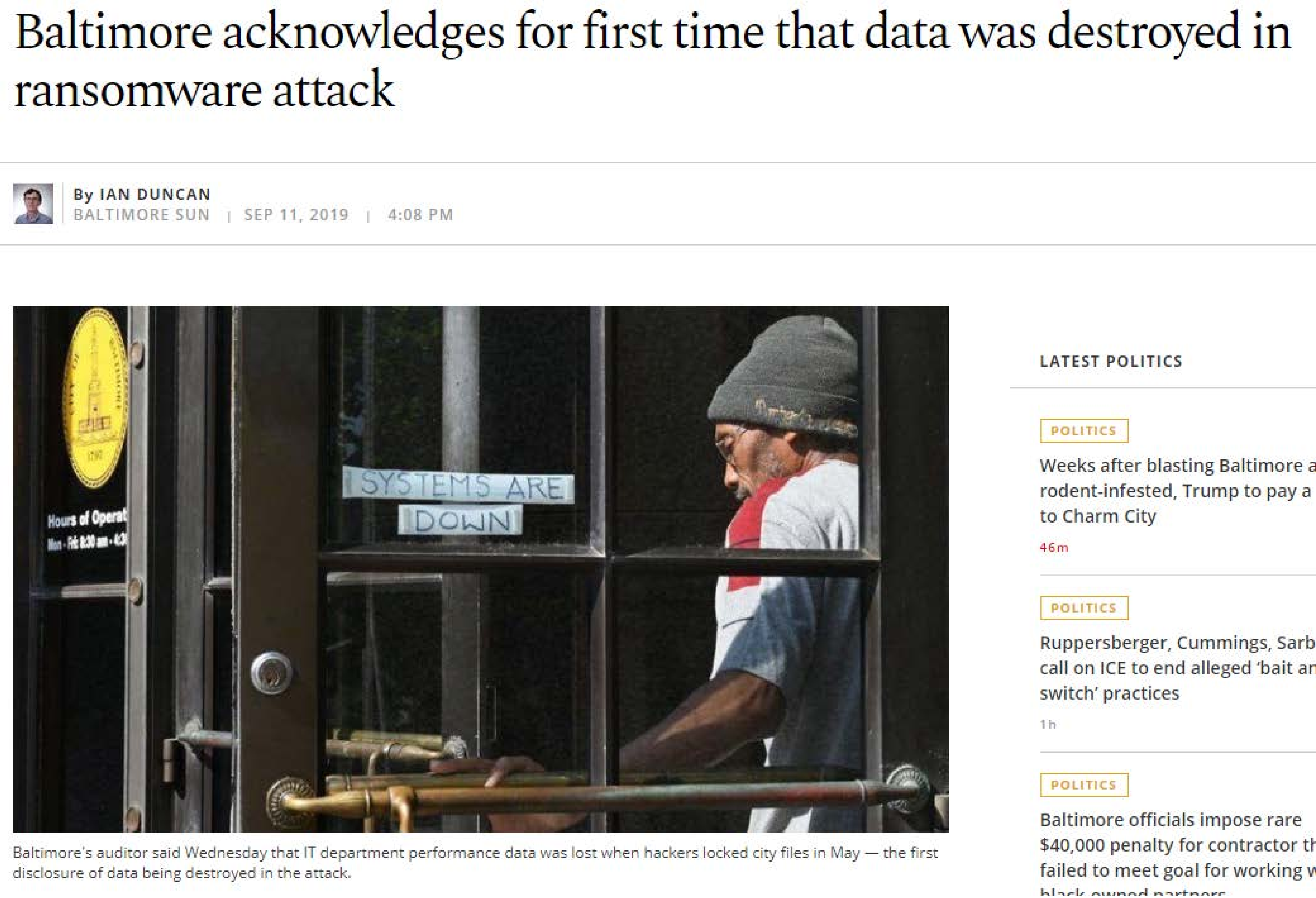


CONFIDENTIAI
Atlanta's cyber a
cost taxpayers

City cyberattack could cost taxpay

1 minute left

A cyber expert says the report shows the city was forced to make drastic change



Baltimore acknowledges for first time that data was destroyed in ransomware attack

By IAN DUNCAN
BALTIMORE SUN | SEP 11, 2019 | 4:08 PM

Baltimore's auditor said Wednesday that IT department performance data was lost when hackers locked city files in May — the first disclosure of data being destroyed in the attack.

LATEST POLITICS

POLITICS

Weeks after blasting Baltimore a
rodent-infested, Trump to pay a
to Charm City

46m

POLITICS

Ruppersberger, Cummings, Sarb
call on ICE to end alleged 'bait ar
switch' practices

1h

POLITICS

Baltimore officials impose rare
$40,000 penalty for contractor th
failed to meet goal for working w
black-owned partners

Questions

Do you lock your door at home?

Have you ever been robbed?

If not, why do you lock your doors?

BACKUP YOUR DATA!

https://www.safeinflorida.com/

Backups (Personal)

1) buy a storage device

2) connect to your computer

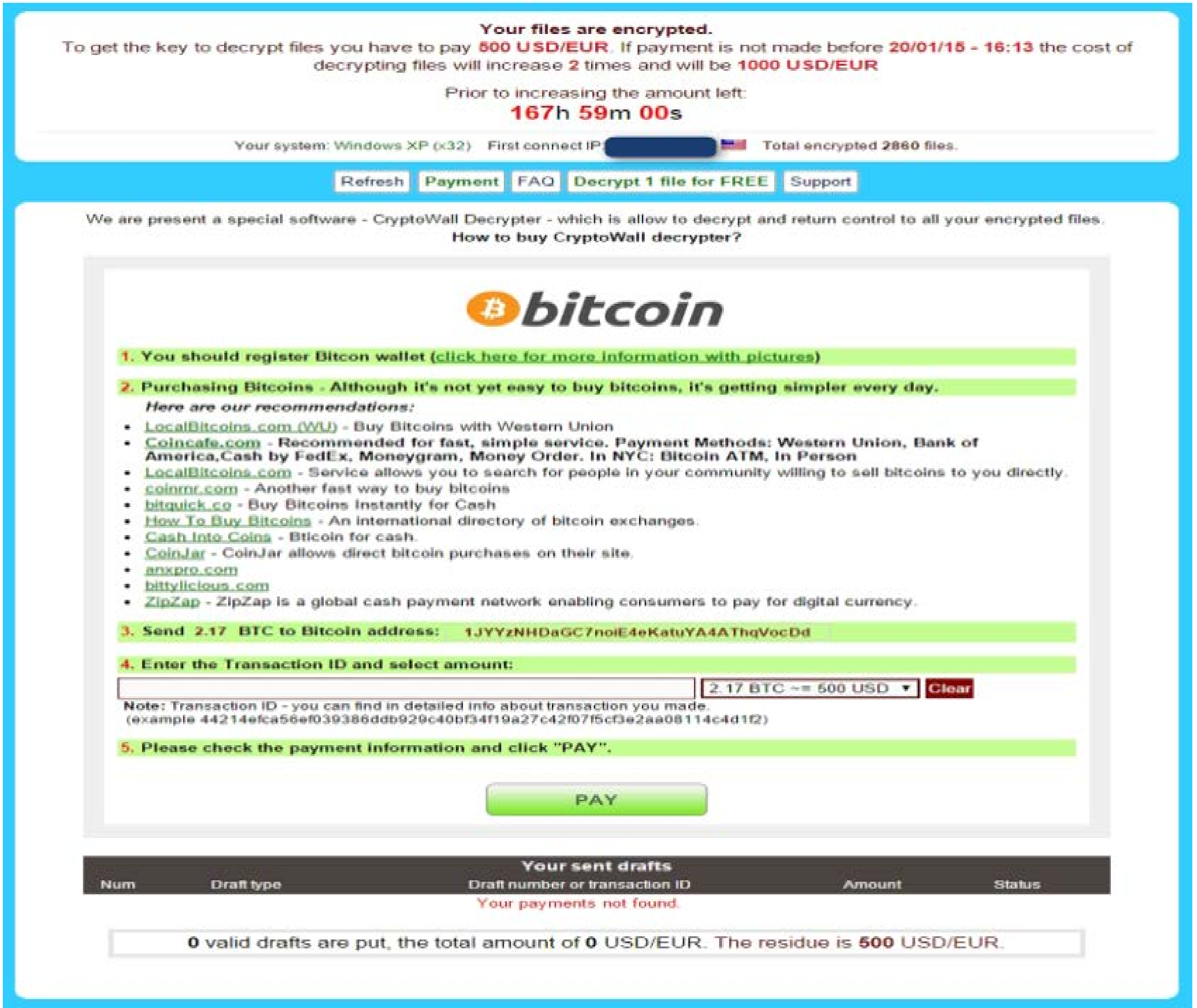
3) copy files to it

4) disconnect from computer

5) repeat on a schedule

4 TB = ~$100

Ransomware Examples



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/01/15 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

167h **59**m **00**s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted **2860** files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 2.17 BTC to Bitcoin address: 1JYYzNHDaGC7noiE4eKatuYA4AThqVocDd

4. Enter the Transaction ID and select amount:

2.17 BTC ~= 500 USD ▾ Clear

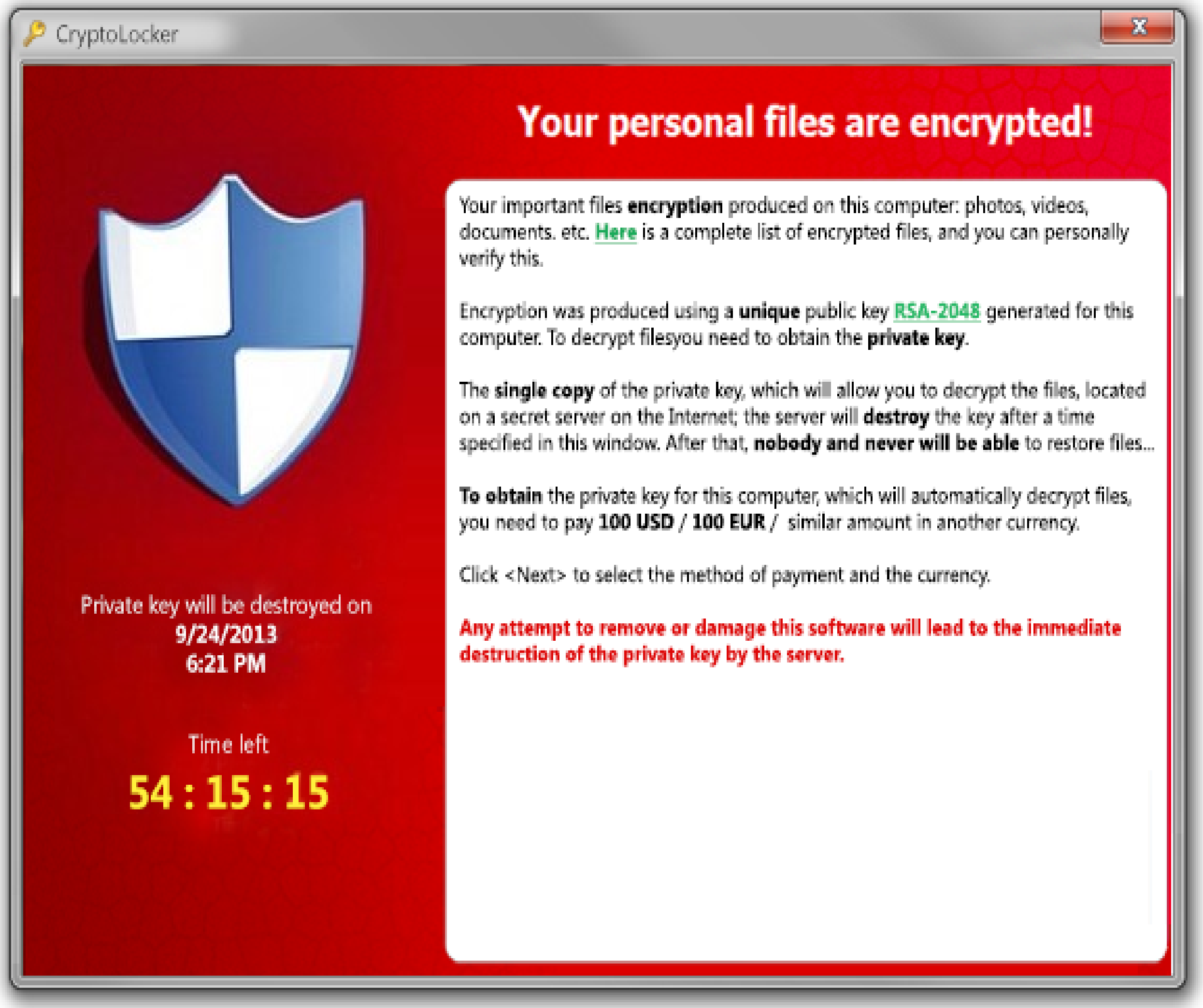
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.



Your personal files are encrypted!

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

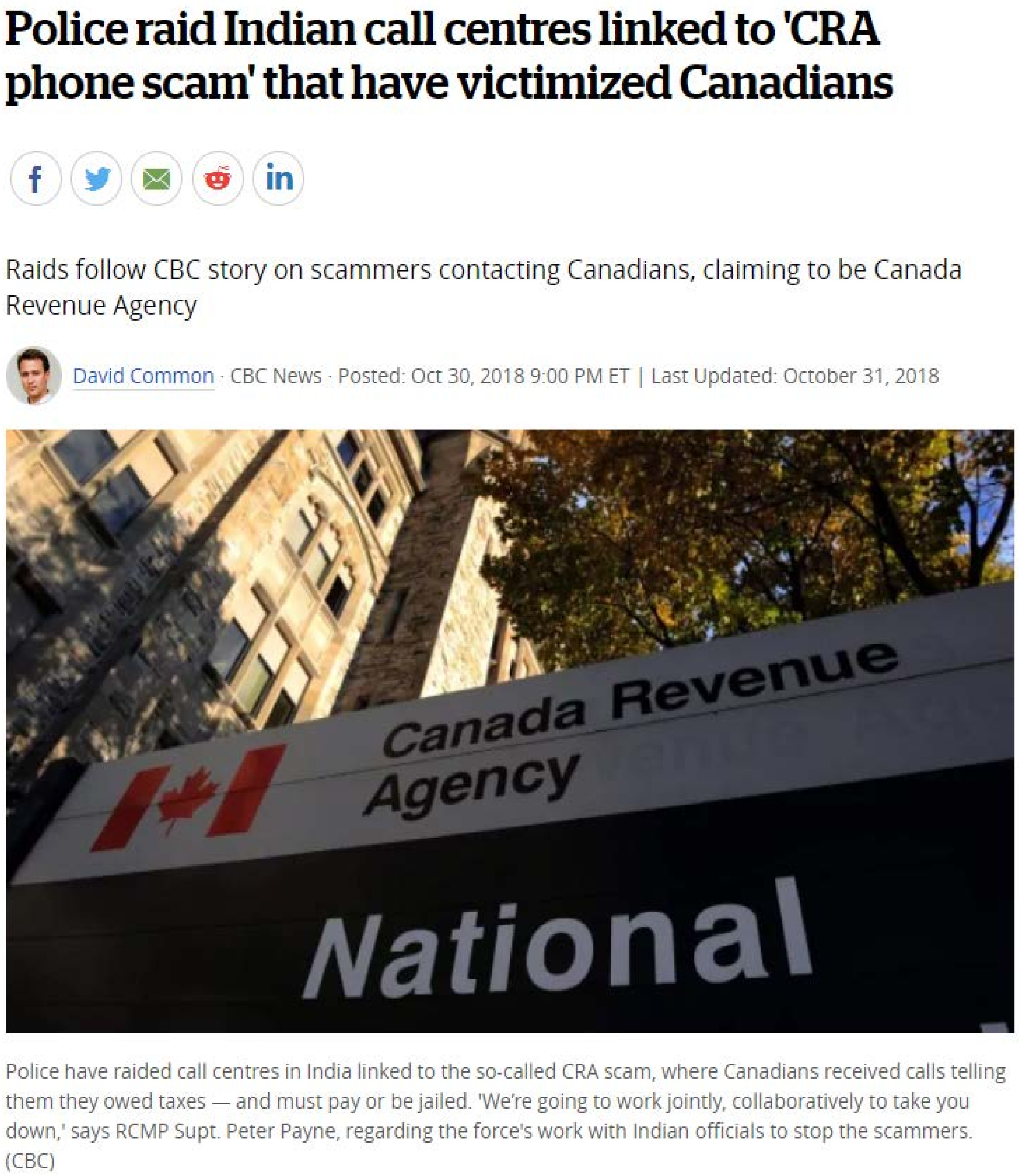
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Ransomware Remedies

Example: RCMP or CRA Scam

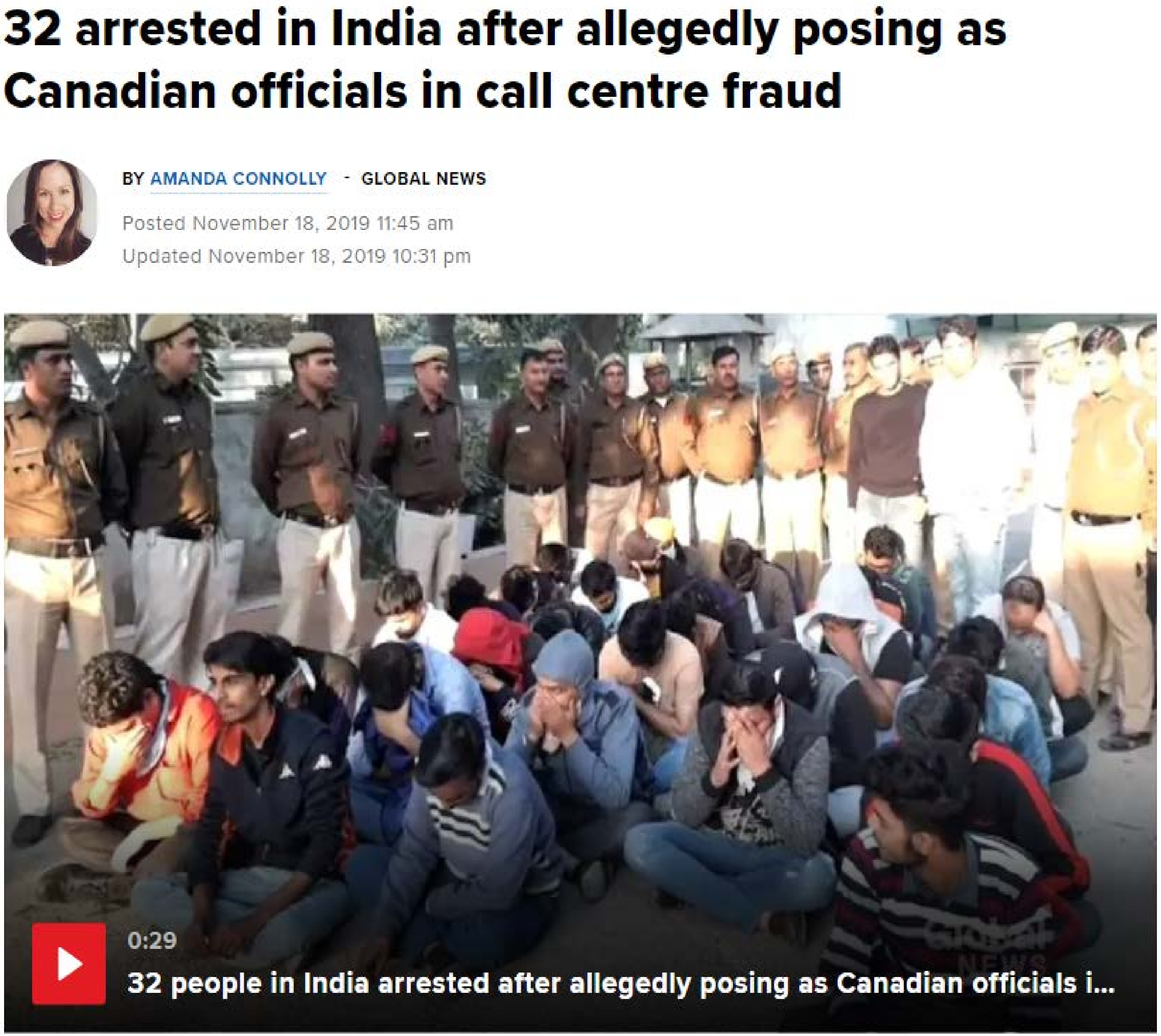


Police raid Indian call centres linked to 'CRA phone scam' that have victimized Canadians

Raids follow CBC story on scammers contacting Canadians, claiming to be Canada Revenue Agency

David Common · CBC News · Posted: Oct 30, 2018 9:00 PM ET | Last Updated: October 31, 2018

Police have raided call centres in India linked to the so-called CRA scam, where Canadians received calls telling them they owed taxes — and must pay or be jailed. 'We're going to work jointly, collaboratively to take you down,' says RCMP Supt. Peter Payne, regarding the force's work with Indian officials to stop the scammers. (CBC)



32 arrested in India after allegedly posing as Canadian officials in call centre fraud

BY AMANDA CONNOLLY · GLOBAL NEWS

Posted November 18, 2019 11:45 am
Updated November 18, 2019 10:31 pm

0:29
32 people in India arrested after allegedly posing as Canadian officials i...

Summary & Call to Action

- humans are doing this to humans
  - social engineering still prevalent

- not a victimless crime
  - victims are often not the firm breached but their customers

- call to action
  - spread the word – get it out there
  - tell 15 people and tell them to tell 15 people

Week 1: 50
Week 2: 750
Week 3: 11,250
Week 4: 168,750
Week 5: 2,531,250
Week 6: 37,968750

Next Generation of Talent

- 3.5 million global shortage of security professionals forecasted by 2021
- 3 million global shortage estimated now
- many jobs, challenging/rewarding, good salary, benefits, coworkers, technology…
- no other industry will help you get started as much….