Grant Thornton

An instinct for growth™

Where's the risk?

Cybersecurity and the impact of COVID-19 on your business

Leah White

Partner

Three areas of focus for today

- Cybersecurity – what is it and why should you care?
- How are hackers breaking in? Real world stories.
- What can you do to protect yourself and your organization? A simple approach to cybersecurity.

Cybersecurity – what is it and why should you care?

What is cybersecurity?

Simply put…

- It's about protecting your network and data from attacks.

Even more importantly, cybersecurity is not…

- an IT issue
- a big business problem
- all about software (e.g., antivirus)

Did you know?

- 71% of Canadian organizations were impacted by a cyber-attack in 2019
- Only 19% of Canadians would continue to do business with an organization if their personal data was exposed in a cyber-attack
- Cyber crime is bigger than illegal drug trafficking as a criminal moneymaker
- And…nearly half of all businesses are putting themselves in the firing line with no strategy to prevent digital crime

** 2019 Cybersecurity Survey Report - Canadian Internet Registration Authority*

Weakest link

People and their curiosity

So why is human error so common?

- A mistaken belief that antivirus and firewalls completely protect them
- Emails that are specifically addressed to them
- Emails about topics that seem relevant (eg. security alerts, invoice payments, etc.)
- Mistakes happen – rushed, not paying attention

1 in 10

URLs being sent have malicious intent

48% of malicious email attachments are Office files – up from 5% in 2017

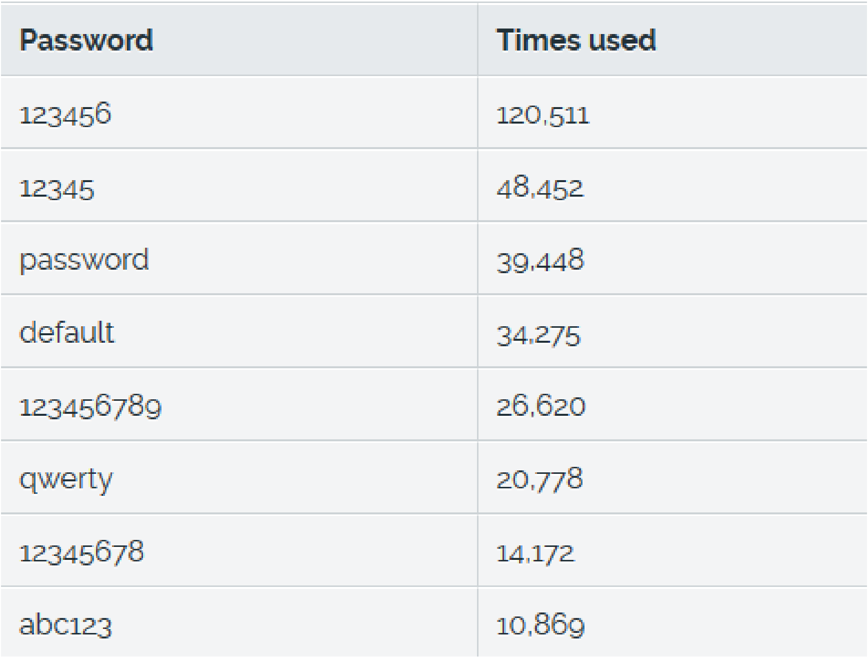
**Symantec 2019 Internet Security Threat Report.*

Weakest link

And it's not just about clicking on the wrong thing…

Worst passwords from the Ashley Madison hack.

And (what a surprise!), they are about as inventive and easy to crack as 123456!



Password	Times used
123456	120,511
12345	48,452
password	39,448
default	34,275
123456789	26,620
qwerty	20,778
12345678	14,172
abc123	10,869

What we are seeing

Cyber awareness is very low for both management and employees

Most of the victims had no real understanding of the full impact that an attack would have on their operations

Low level of knowledge on cyber insurance

Most victim organizations did not have appropriate data backup

Many victims placed undue reliance on underqualified outsourced IT contractors

Almost all victims had not taken even the easiest logical steps to enhance their security

In more sophisticated hacks, time to discovery is months or longer

An alarming number of victims did not have commercial AV software

Cybersecurity and hospitality

You're probably all familiar with the Marriott data breach …

- – Exposed the personal information of 339 million guests
- – Projected to cost Marriott billions of dollars

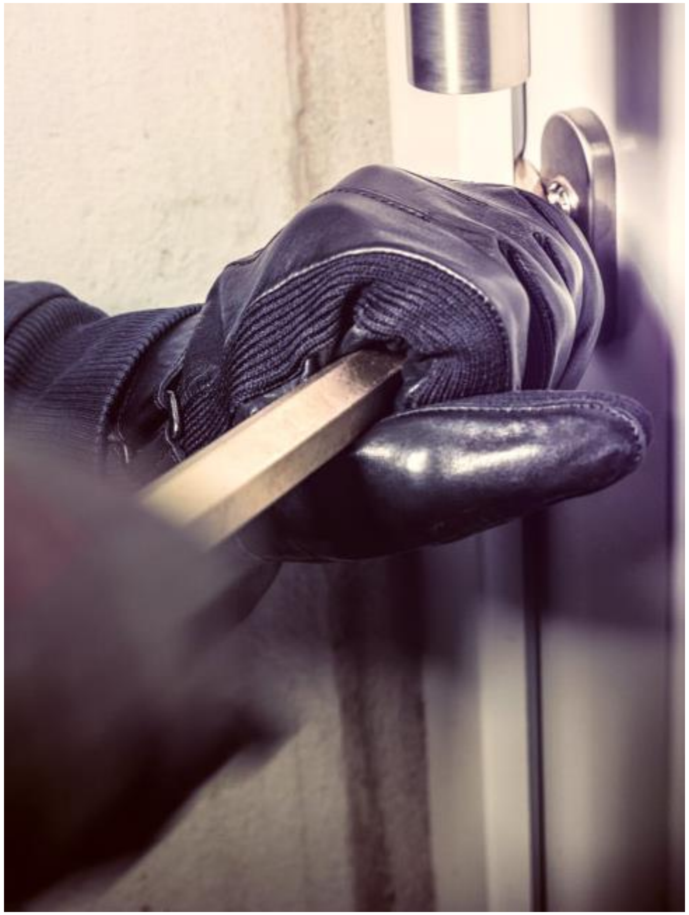
- 9% of consumers said they were victims of hotel breaches and 10% said they were victims of restaurant breaches
- 70% of guests don't think the hotels are they stay at are doing enough for cybersecurity
- Millennials believe Airbnb is less vulnerable to a cyberattack than a traditional hotel
- 49% of women and 42% of men say that trust in a hotel's cybersecurity influences whether they book with them
- 40% of hotel guests were worried about breaches of the hotel's WiFi

** 2019 MORPHISEC Hospitality Guest Cybersecurity Threat Index*

How are hackers breaking in? Real world stories.

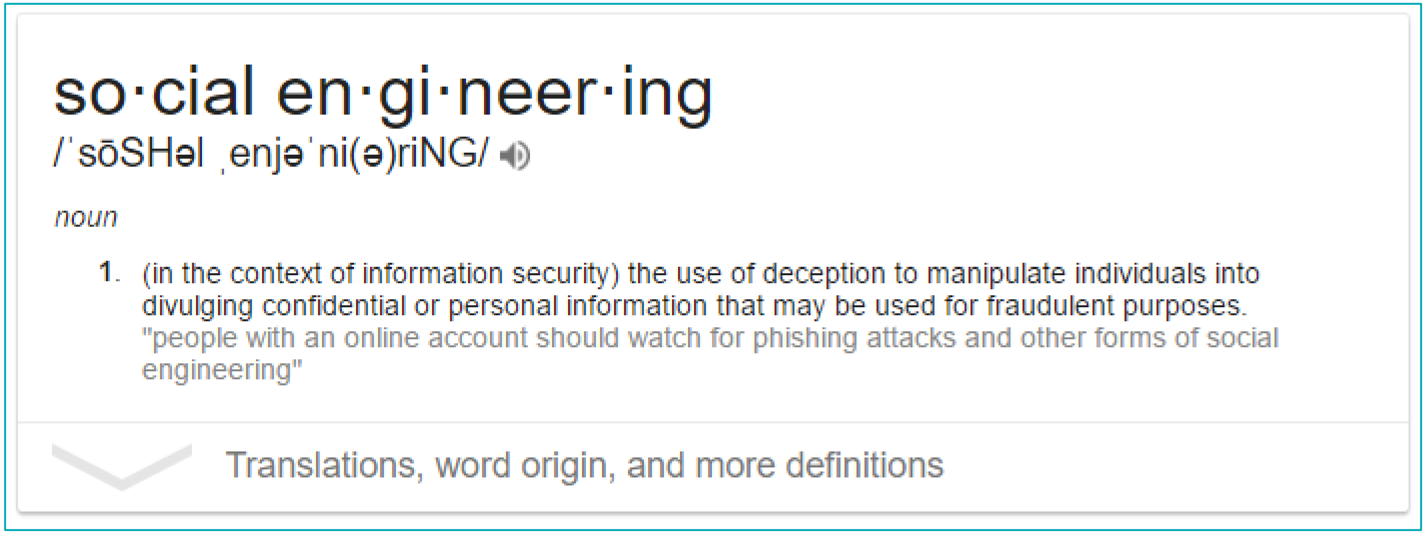
Types of cyber attacks

- Social engineering
- Phishing and spear phishing
- Ransomware
- Malware
- Mobile malware
- Waterhole attacks



Social engineering

- The art of gaining access by exploiting human psychology, rather than by breaking in or using technical hacking techniques
- More than 60% of businesses were victims of social engineering attacks last year



so·cial en·gi·neer·ing

/ˈsōSHəl ˌenjəˈni(ə)riNG/

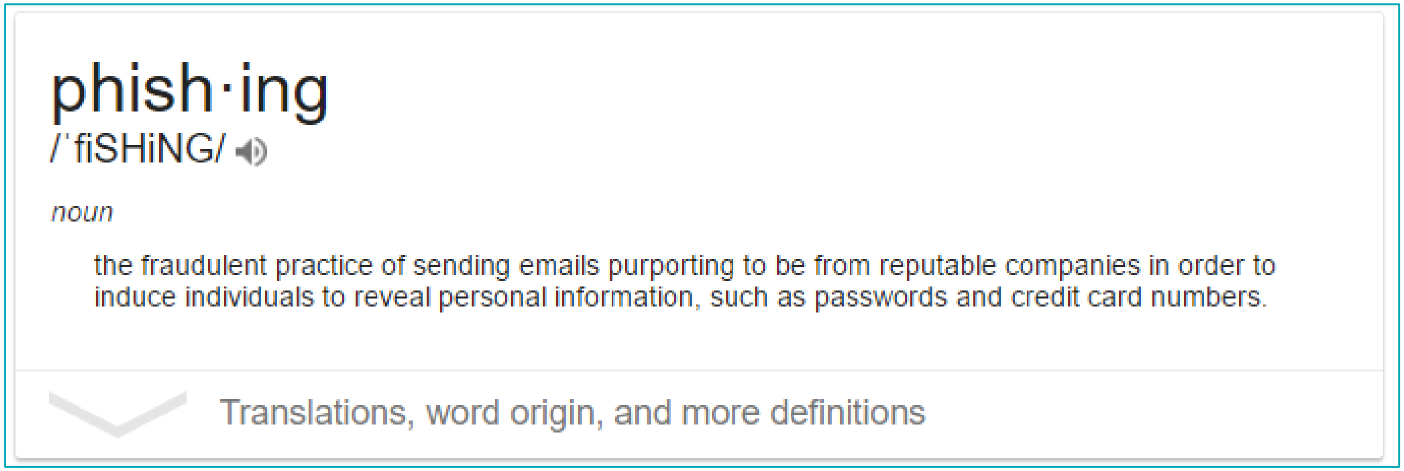
noun

1. (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
"people with an online account should watch for phishing attacks and other forms of social engineering"

SIM swapping/cell phone porting

- We're relying on our cell phones even more
- Hackers are using data exposed through data breaches to contact cell phone providers and steal your cell phone number
- They can then use this to reset your passwords to your email, PayPal, etc. and start making purchases with your accounts
- Harder to fix during a pandemic if you no longer have access to your phone

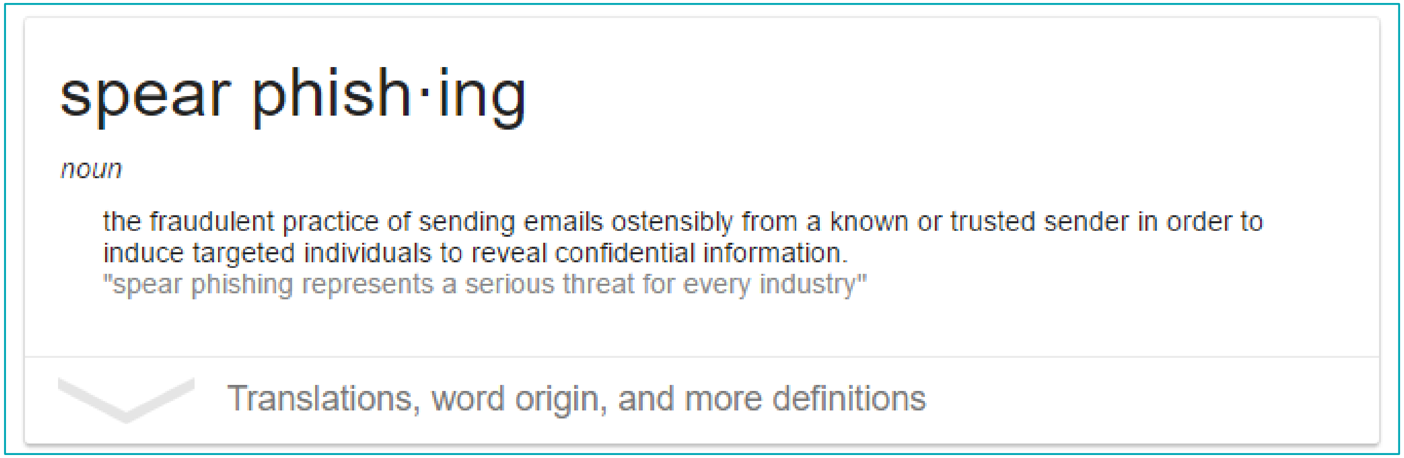
Phishing and spear phishing



phish·ing
/ˈfiSHiNG/

noun

the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

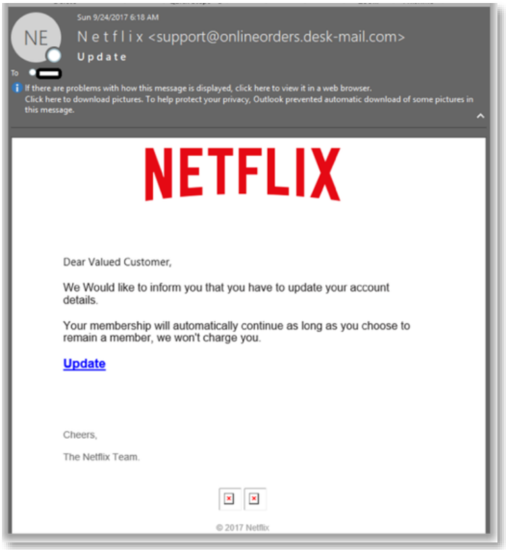


spear phish·ing

noun

the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.
"spear phishing represents a serious threat for every industry"

Phishing



Sun 9/24/2017 6:18 AM

Netflix <support@onlineorders.desk-mail.com>

Update

To [redacted]

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.

NETFLIX

Dear Valued Customer,

We Would like to inform you that you have to update your account details.

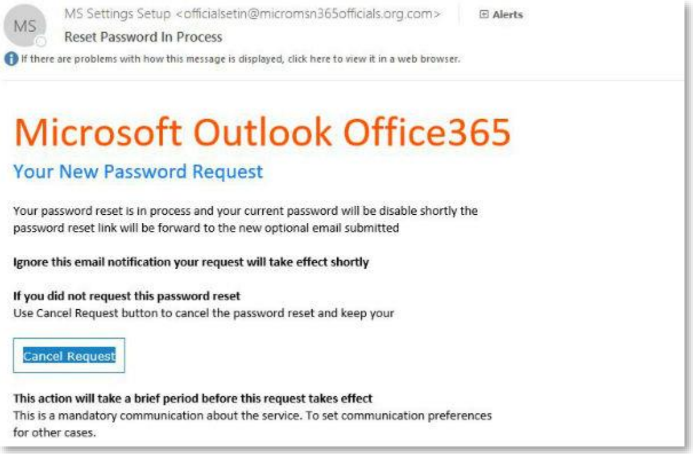
Your membership will automatically continue as long as you choose to remain a member, we won't charge you.

Update

Cheers,

The Netflix Team.

© 2017 Netflix



MS Settings Setup <officialsetin@micromsn365officials.org.com>

Reset Password In Process

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft Outlook Office365

Your New Password Request

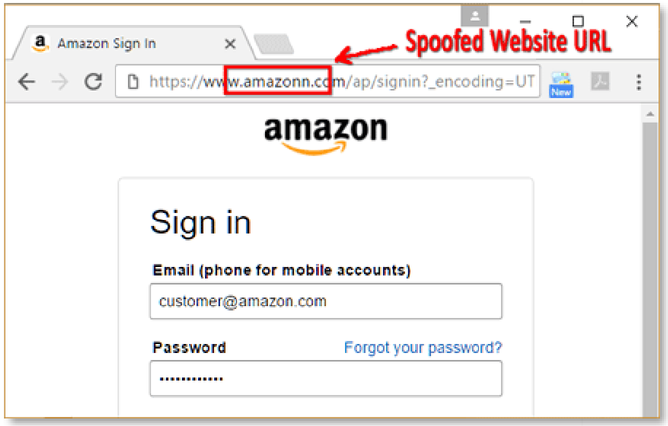
Your password reset is in process and your current password will be disable shortly the password reset link will be forward to the new optional email submitted

Ignore this email notification your request will take effect shortly

If you did not request this password reset
Use Cancel Request button to cancel the password reset and keep your

Cancel Request

This action will take a brief period before this request takes effect
This is a mandatory communication about the service. To set communication preferences for other cases.



https://www.amazonn.com/ap/signin?_encoding=UT

amazon

Sign in

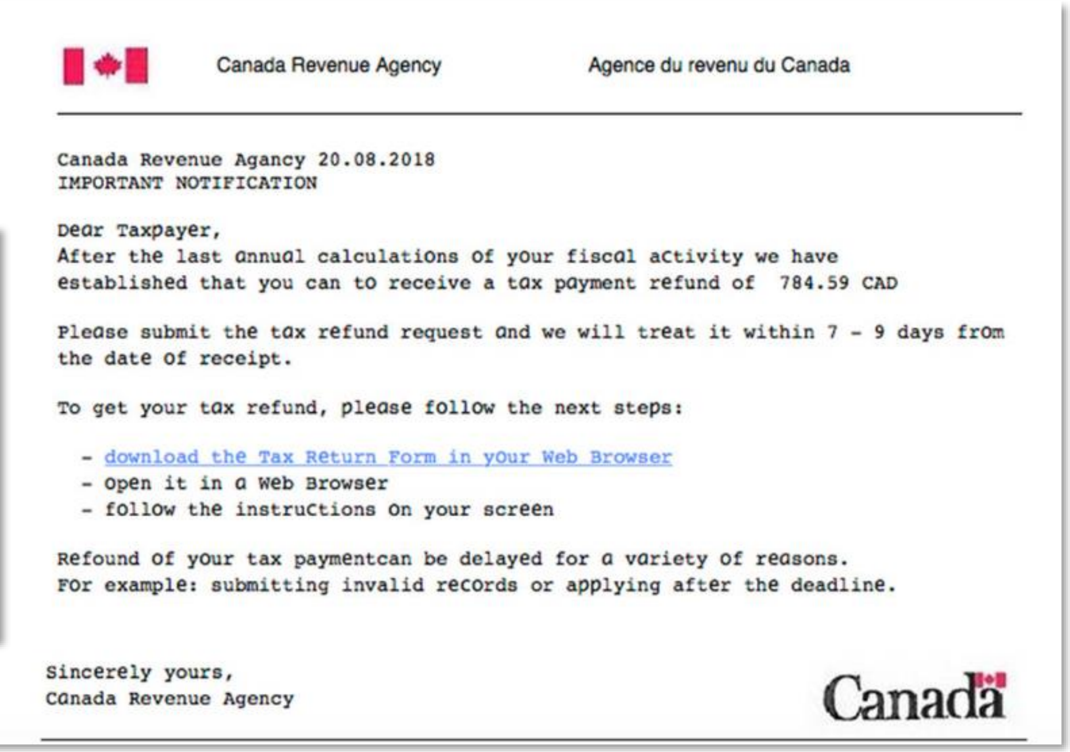
Email (phone for mobile accounts)

customer@amazon.com

Password

Forgot your password?

....



Canada Revenue Agency Agence du revenu du Canada

Canada Revenue Agancy 20.08.2018
IMPORTANT NOTIFICATION

Dear Taxpayer,
After the last annual calculations of your fiscal activity we have established that you can to receive a tax payment refund of 784.59 CAD

Please submit the tax refund request and we will treat it within 7 - 9 days from the date of receipt.

To get your tax refund, please follow the next steps:

- download the Tax Return Form in your Web Browser
- open it in a Web Browser
- follow the instructions on your screen

Refound of your tax paymentcan be delayed for a variety of reasons.
For example: submitting invalid records or applying after the deadline.

Sincerely yours,
Canada Revenue Agency

Canada

Phishing

How do hackers convince you to click on things?

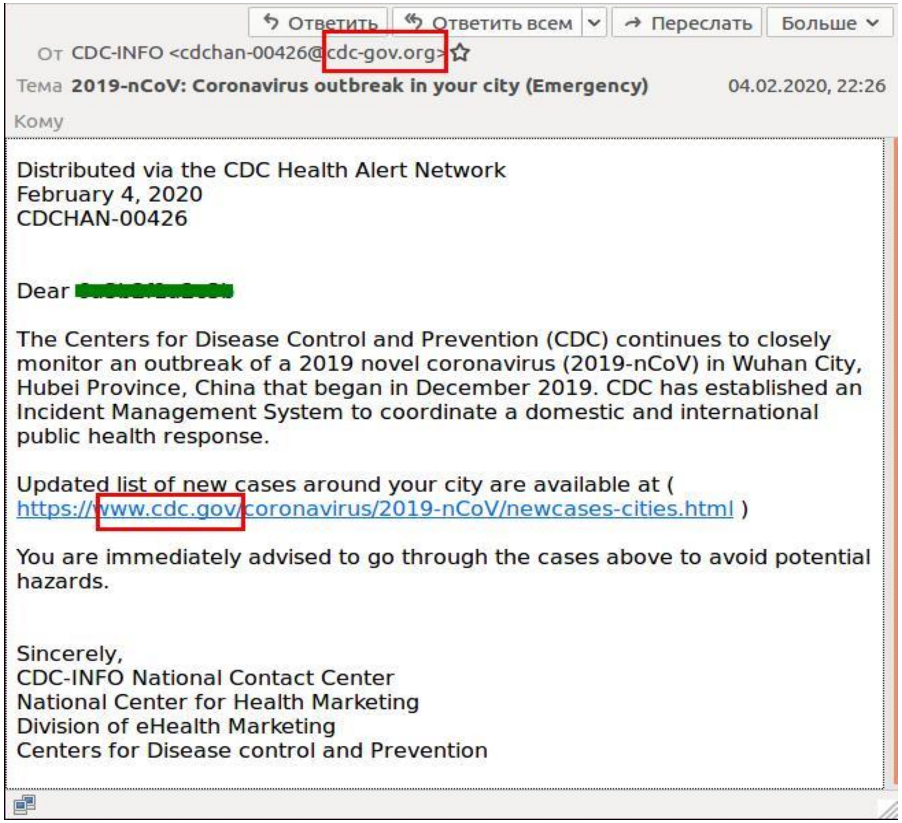
- Curiosity – Making the topic interesting/appealing
- Pressure – Creating a sense of urgency
- Context – Making the topic relevant to the current environment

So what does this look like in the pandemic environment?

- Curiosity – People are hungry for information about the virus
- Pressure – People are scared, and hackers can prey on this fear
- Context – Topics can be linked to recent pandemic developments

Phishing

…let’s look at an example



От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

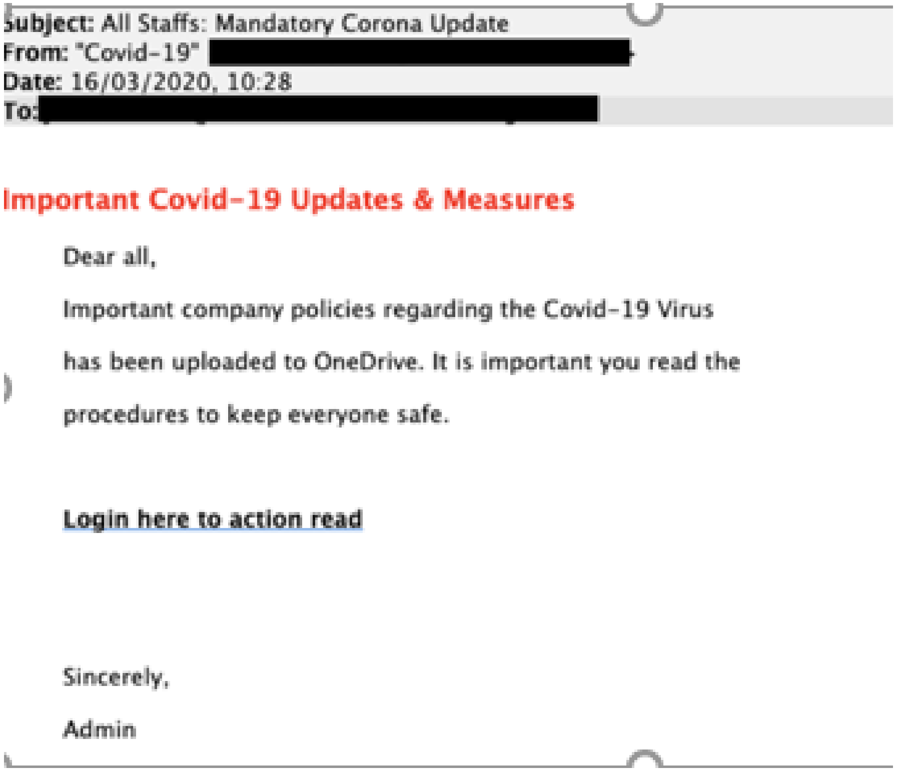
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

The growing threat of hackers

And yet another…



Subject: All Staffs: Mandatory Corona Update
From: "Covid-19" [redacted]
Date: 16/03/2020, 10:28
To: [redacted]

Important Covid-19 Updates & Measures

Dear all,

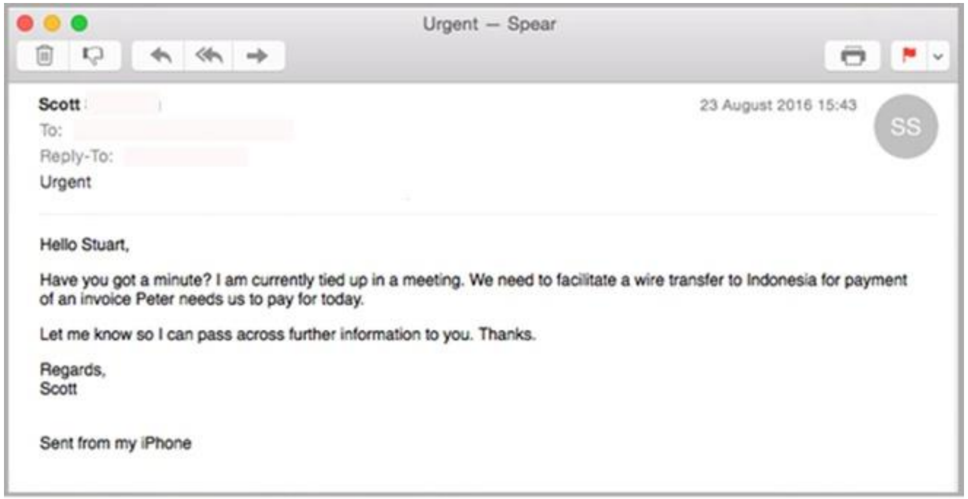
Important company policies regarding the Covid-19 Virus has been uploaded to OneDrive. It is important you read the procedures to keep everyone safe.

Login here to action read

Sincerely,

Admin

Spear phishing



Scott [redacted]
To: [redacted]
Reply-To: [redacted]
Urgent

23 August 2016 15:43

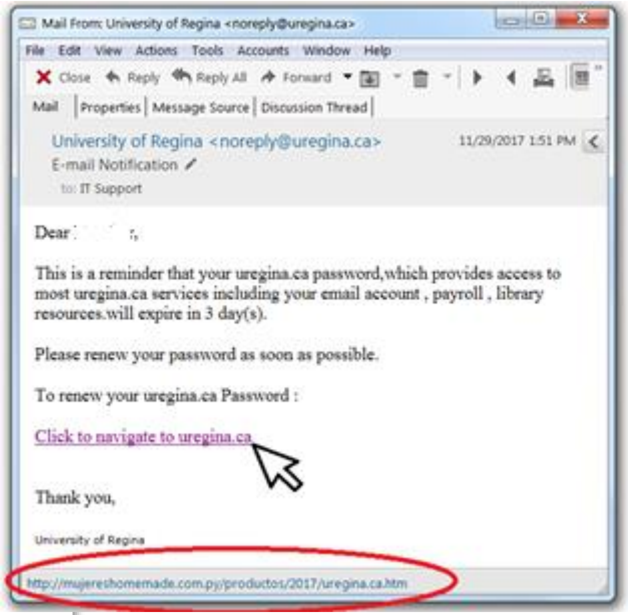
Hello Stuart,

Have you got a minute? I am currently tied up in a meeting. We need to facilitate a wire transfer to Indonesia for payment of an invoice Peter needs us to pay for today.

Let me know so I can pass across further information to you. Thanks.

Regards,
Scott

Sent from my iPhone



Mail From: University of Regina <noreply@uregina.ca>
File Edit View Actions Tools Accounts Window Help
Close Reply Reply All Forward
Mail Properties Message Source Discussion Thread

University of Regina <noreply@uregina.ca>
E-mail Notification
to: IT Support

11/29/2017 1:51 PM

Dear [redacted],

This is a reminder that your uregina.ca password,which provides access to most uregina.ca services including your email account , payroll , library resources.will expire in 3 day(s).

Please renew your password as soon as possible.

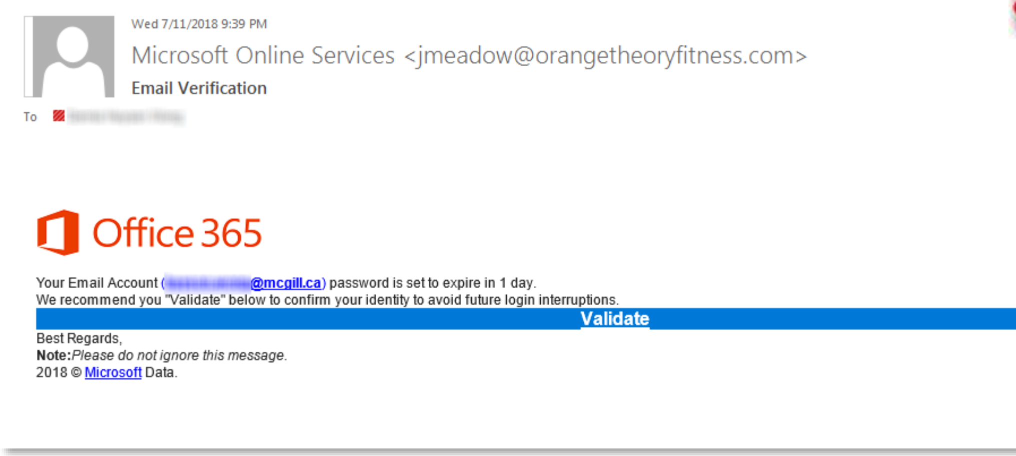
To renew your uregina.ca Password :

Click to navigate to uregina.ca

Thank you,

University of Regina

http://mujereshomemade.com.py/productos/2017/uregina.ca.htm



Wed 7/11/2018 9:39 PM

Microsoft Online Services <jmeadow@orangetheoryfitness.com>

Email Verification

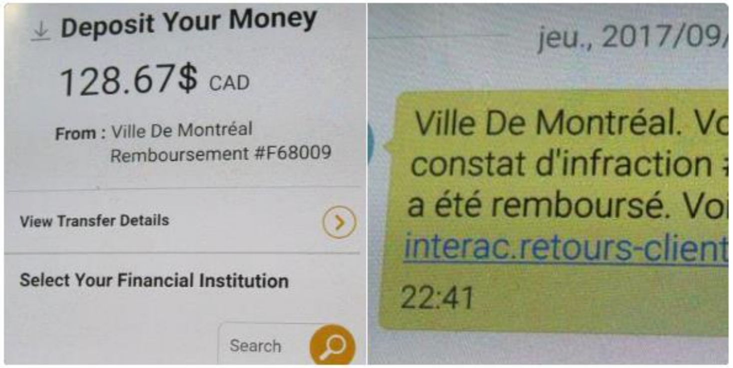
To [redacted]

Office 365

Your Email Account ([redacted]@mcgill.ca) password is set to expire in 1 day.
We recommend you "Validate" below to confirm your identity to avoid future login interruptions.

Best Regards,
Note:*Please do not ignore this message.*
2018 © Microsoft Data.

Mobile phishing or smishing



Deposit Your Money

128.67$ CAD

From : Ville De Montréal
Remboursement #F68009

View Transfer Details

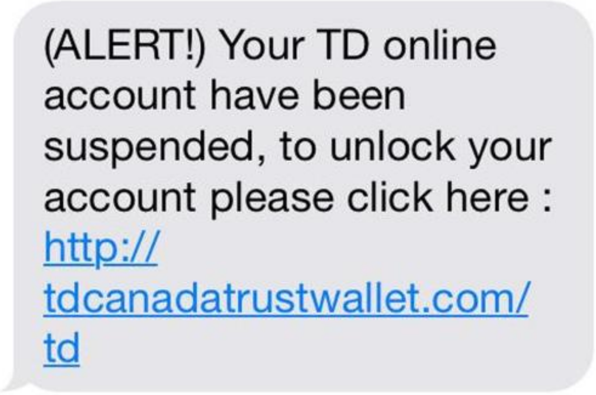
Select Your Financial Institution

Search

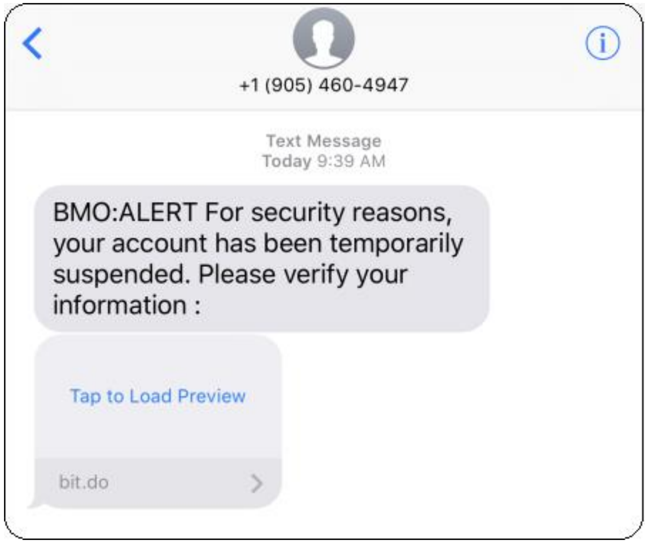
jeu., 2017/09/

Ville De Montréal. Vo
constat d'infraction
a été remboursé. Voi
interac.retours-client

22:41



(ALERT!) Your TD online account have been suspended, to unlock your account please click here : http://tdcanadatrustwallet.com/td



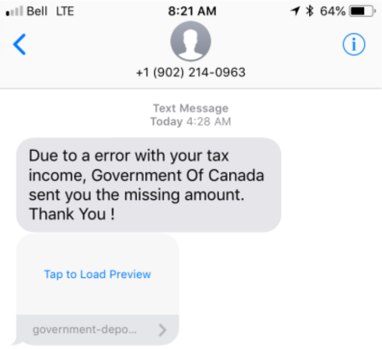
+1 (905) 460-4947

Text Message
Today 9:39 AM

BMO:ALERT For security reasons, your account has been temporarily suspended. Please verify your information :

Tap to Load Preview

bit.do



Bell LTE 8:21 AM 64%

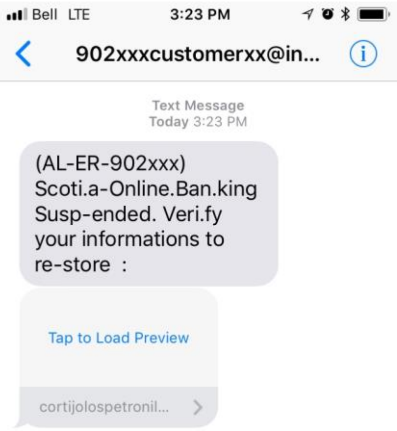
+1 (902) 214-0963

Text Message
Today 4:28 AM

Due to a error with your tax income, Government Of Canada sent you the missing amount. Thank You !

Tap to Load Preview

government-depo...



Bell LTE 3:23 PM

902xxxcustomerxx@in...

Text Message
Today 3:23 PM

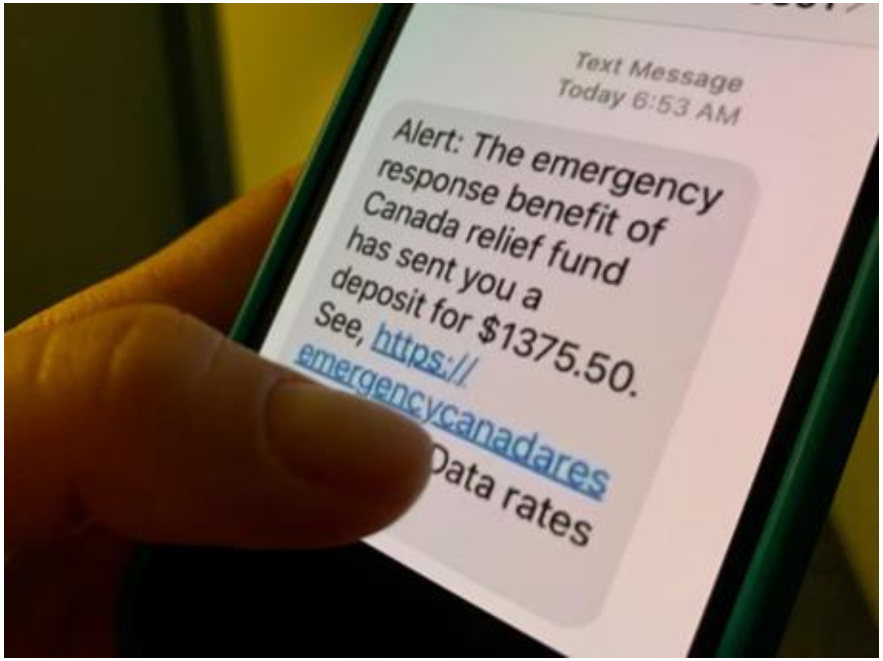
(AL-ER-902xxx) Scoti.a-Online.Ban.king Susp-ended. Veri.fy your informations to re-store :

Tap to Load Preview

cortijolospetronil...

Mobile phishing or smishing

And hackers are using the pandemic here too…



Text Message
Today 6:53 AM

Alert: The emergency response benefit of Canada relief fund has sent you a deposit for $1375.50. See, https:// emergencycanadares

Data rates

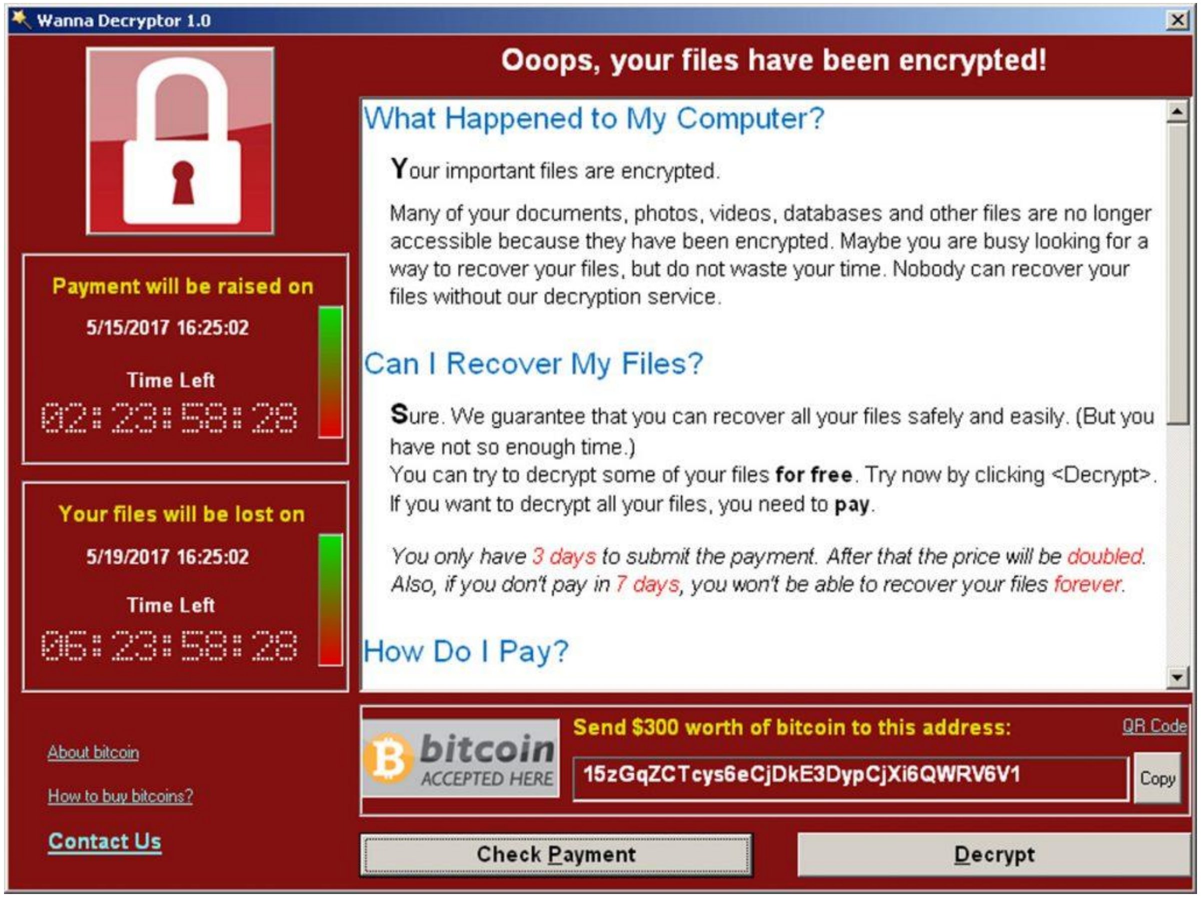
Ransomware

- Malware that blocks access to a victim's files and the only way to gain access is to pay a ransom
- Can only block access by encrypting the files or locking victims out of the operating system

75% of Canadian businesses were inclined to pay an extortion fee pre-pandemic.

**Symantec 2019 Internet Security Threat Report.*

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

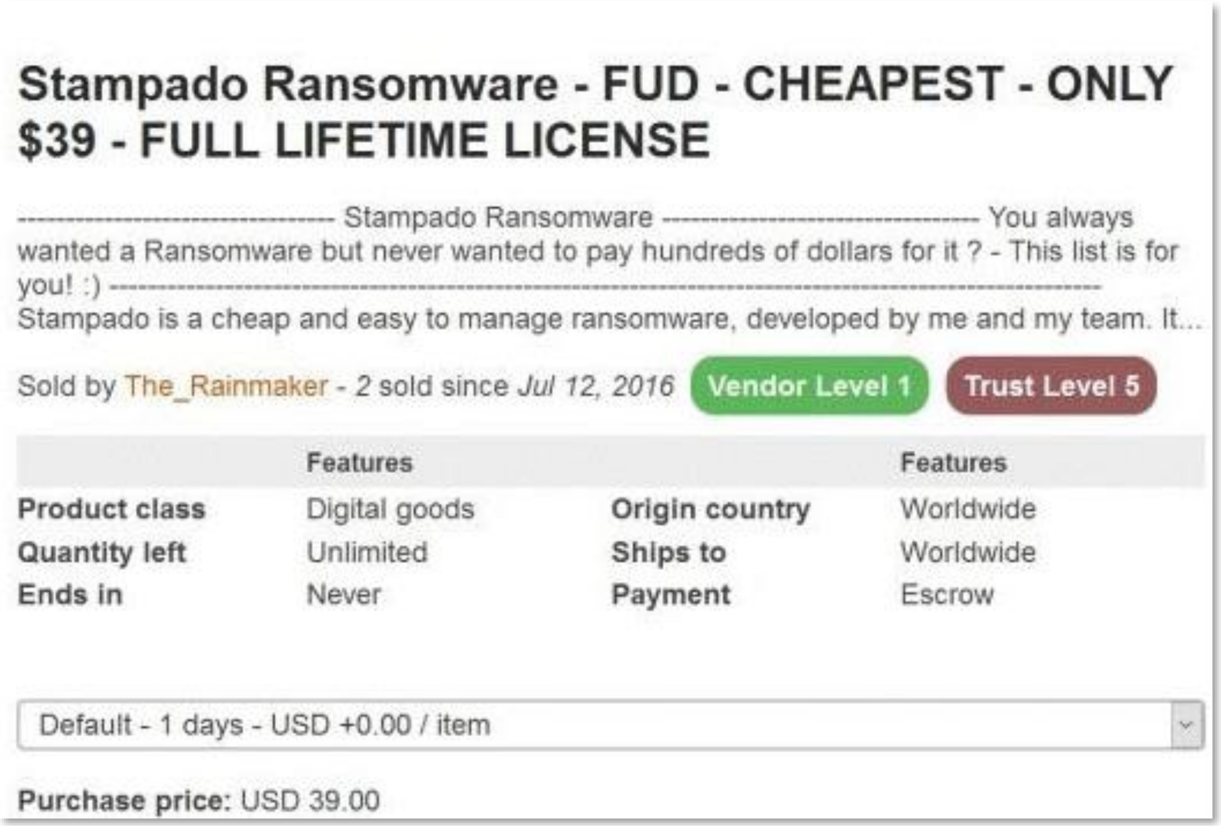
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Ransomware and other tools are cheap



Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - FULL LIFETIME LICENSE

---------------------------------- Stampado Ransomware ---------------------------------- You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :) --
Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by The_Rainmaker - *2* sold since *Jul 12, 2016*

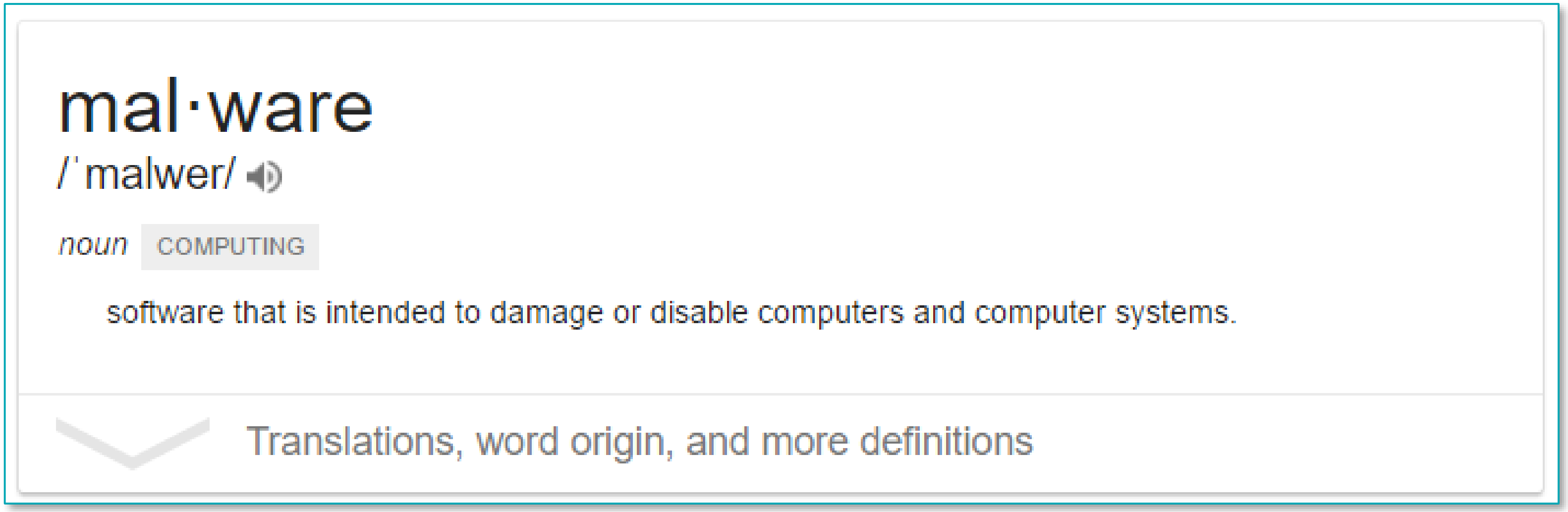
	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

Malware

- Any piece of software that was written with the intent of doing harm to data, devices or to people
- Decline in long running malware types, but mobile versions have grown by **50% recently**



mal·ware

/ˈmalwer/

noun COMPUTING

software that is intended to damage or disable computers and computer systems.

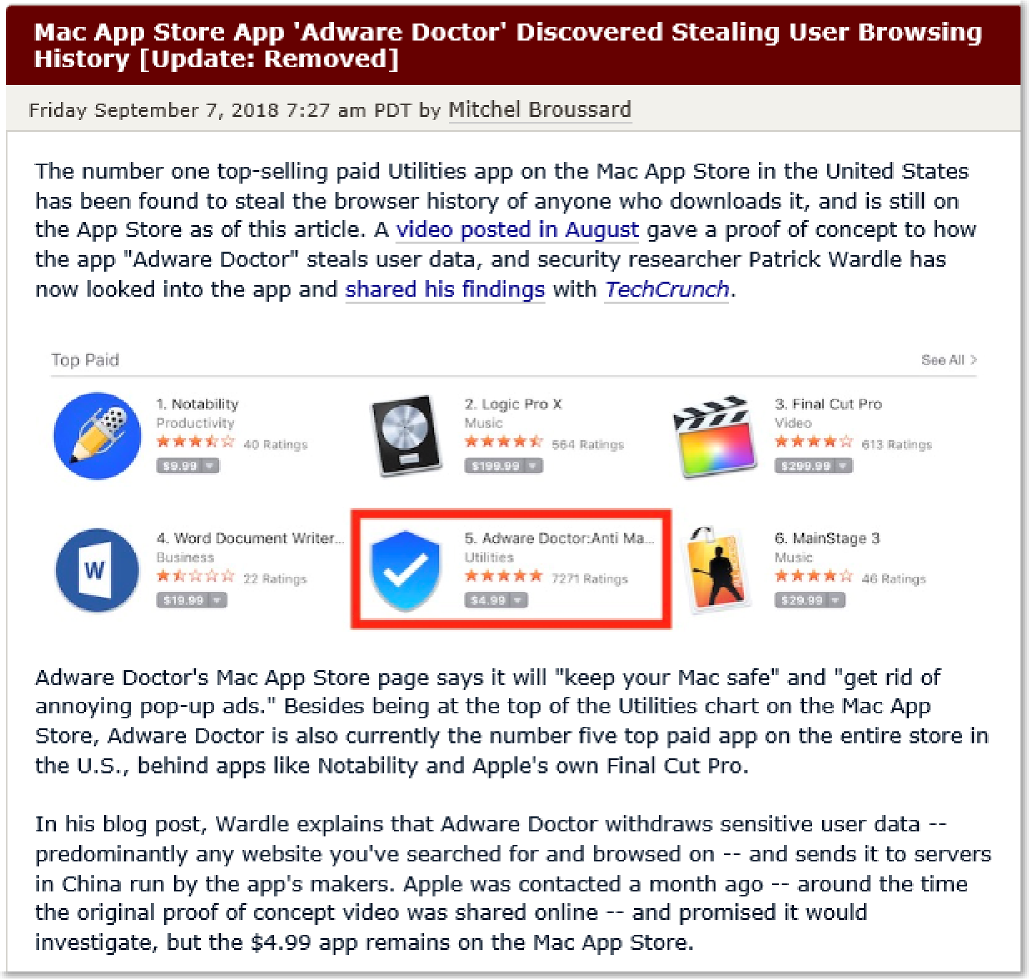
Mobile malware

- Malicious software that is specifically built to attack mobile phone or smartphone systems - causing loss or leakage of confidential information

One in **36** mobile devices have high risk apps installed

**Symantec 2019 Internet Security Threat Report.*

Mobile malware



Mac App Store App 'Adware Doctor' Discovered Stealing User Browsing History [Update: Removed]

Friday September 7, 2018 7:27 am PDT by Mitchel Broussard

The number one top-selling paid Utilities app on the Mac App Store in the United States has been found to steal the browser history of anyone who downloads it, and is still on the App Store as of this article. A video posted in August gave a proof of concept to how the app "Adware Doctor" steals user data, and security researcher Patrick Wardle has now looked into the app and shared his findings with *TechCrunch*.

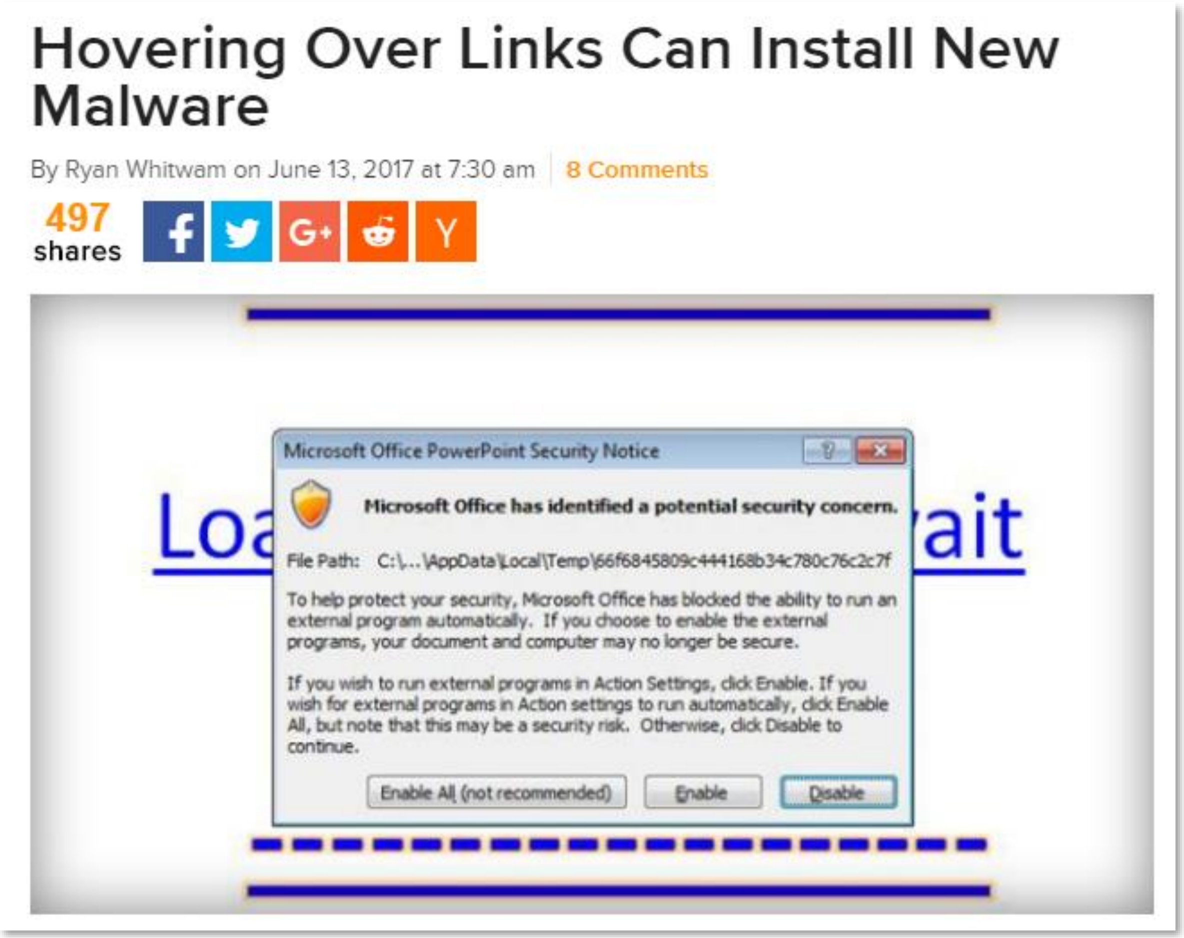
Adware Doctor's Mac App Store page says it will "keep your Mac safe" and "get rid of annoying pop-up ads." Besides being at the top of the Utilities chart on the Mac App Store, Adware Doctor is also currently the number five top paid app on the entire store in the U.S., behind apps like Notability and Apple's own Final Cut Pro.

In his blog post, Wardle explains that Adware Doctor withdraws sensitive user data -- predominantly any website you've searched for and browsed on -- and sends it to servers in China run by the app's makers. Apple was contacted a month ago -- around the time the original proof of concept video was shared online -- and promised it would investigate, but the $4.99 app remains on the Mac App Store.

Malware on public wifi

Free Wi-Fi.
Like free, free.

Malware with links



Hovering Over Links Can Install New Malware

By Ryan Whitwam on June 13, 2017 at 7:30 am | 8 Comments

497 shares

Microsoft Office PowerPoint Security Notice

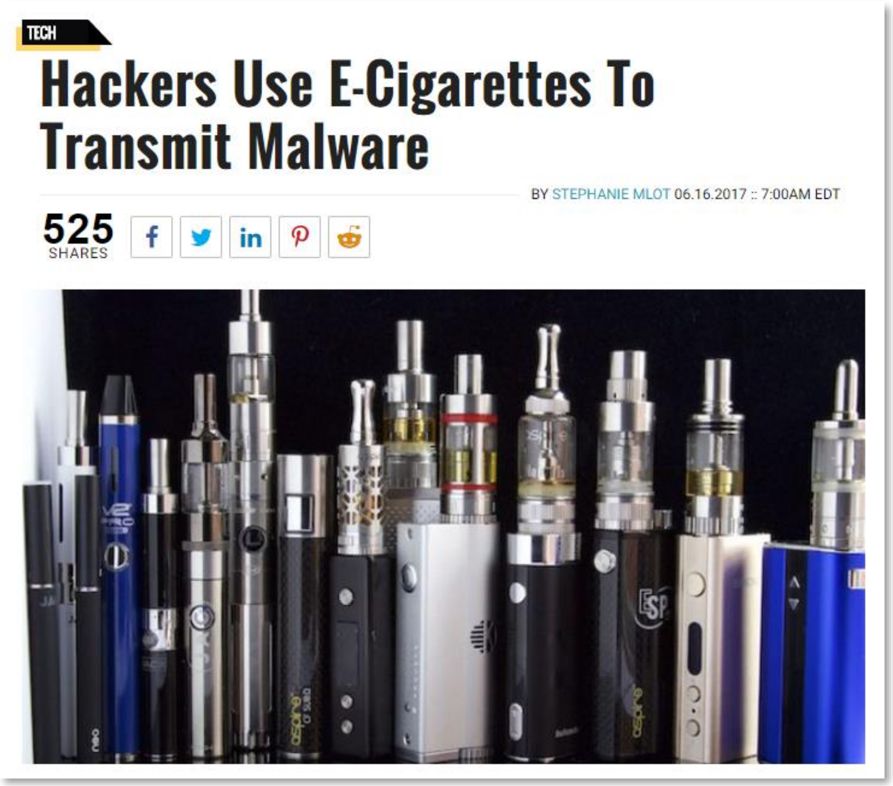
Microsoft Office has identified a potential security concern.

File Path: C:\...\AppData\Local\Temp\66f6845809c444168b34c780c76c2c7f

To help protect your security, Microsoft Office has blocked the ability to run an external program automatically. If you choose to enable the external programs, your document and computer may no longer be secure.

If you wish to run external programs in Action Settings, click Enable. If you wish for external programs in Action settings to run automatically, click Enable All, but note that this may be a security risk. Otherwise, click Disable to continue.

Malware on devices

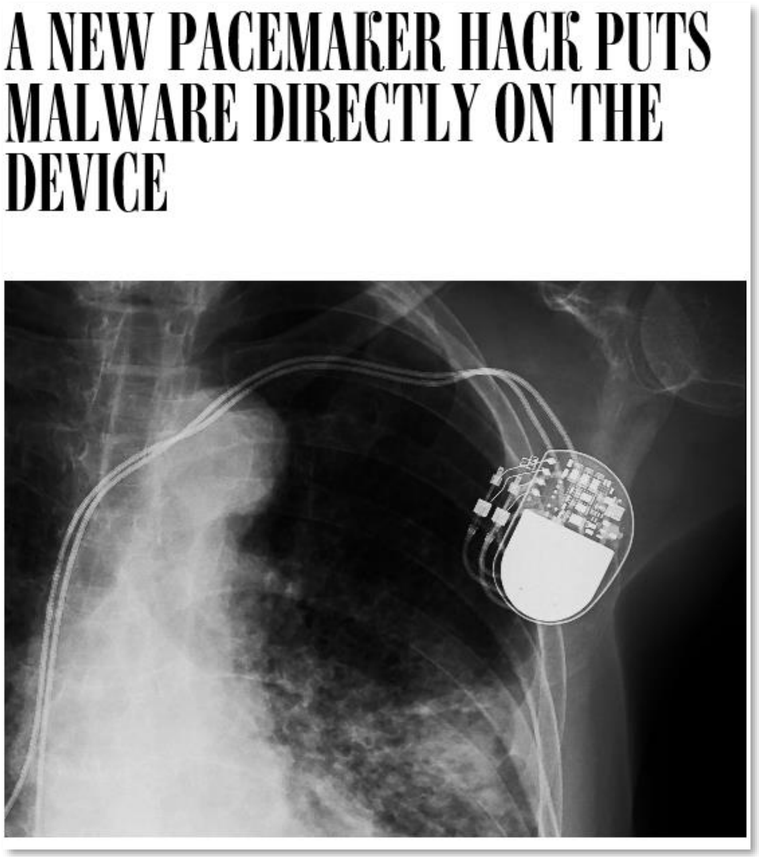


TECH

Hackers Use E-Cigarettes To Transmit Malware

BY STEPHANIE MLOT 06.16.2017 :: 7:00AM EDT

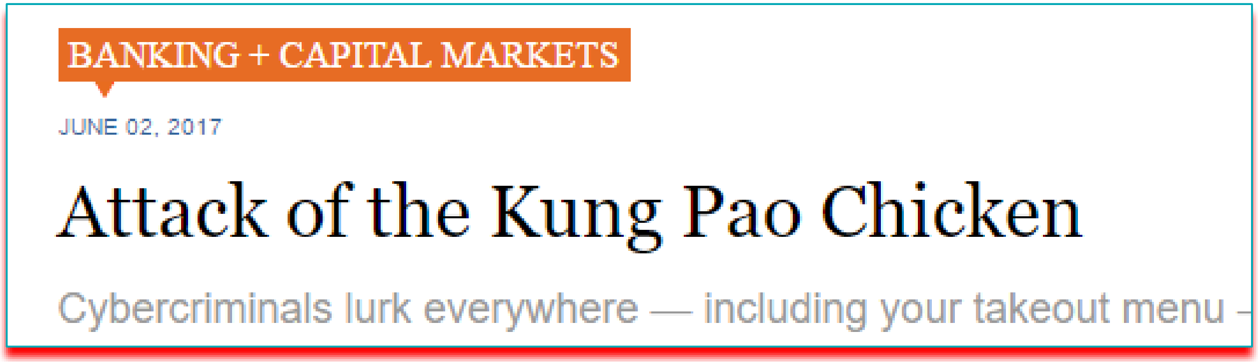
525 SHARES



A NEW PACEMAKER HACK PUTS MALWARE DIRECTLY ON THE DEVICE

Watering hole attacks

- Targeting a specific group of users by infecting websites that groups are known to visit
- Goal is to infect the targeted user's computer and gain access to their network



BANKING + CAPITAL MARKETS

JUNE 02, 2017

Attack of the Kung Pao Chicken

Cybercriminals lurk everywhere — including your takeout menu –

*Symantec 2019 Internet Security Threat Report.

Business email compromise

What is it?

Fraudsters either spoof or take over the account of an executive or finance employee, and send email messages such as:

a. Pretending to be a supplier, and emailing a customer to request a change in bank information to an account controlled by the fraudster (e.g., City of Saskatoon – over $1,000,000 sent to an individual pretending to be the CFO of a local construction company)

b. Pretending to be the CEO or CFO, and requesting that money be transferred to an account the fraudster controls (often through wire transfer). Gift cards is also a common option

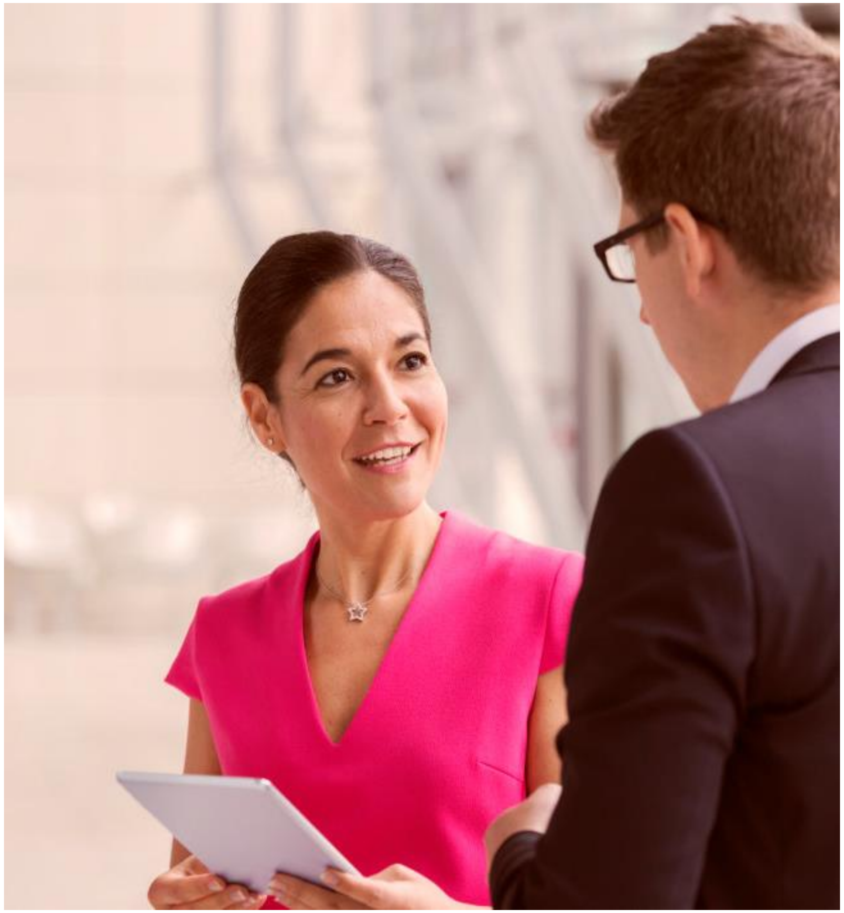
c. Pretending to be an employee, and asking payroll to change their banking information to an account controlled by the fraudster (e.g., Royal Canadian Mint)

What can you do to protect yourself and your organization?

A simple approach to cybersecurity.

Start the Cybersecurity conversation at your organization

- Cybersecurity isn't just a technology issue, it's about business risk, organizational culture, and education



Reducing your risk

Security awareness training for employees

- Onboarding
- Reading a policy is likely not enough
- Consider concepts in behavioral change – easy, rewarding and normal
- Can't just communicate the change – reinforcement is key
- Ensure that passwords are strong – and educate employees not to use the same password across multiple platforms

Reducing your risk

Consider your own IT environment

- Do you run antivirus? Firewalls? Are they current?
- Are your patches up to date?
- What are your IT security policies and procedures?
- How would you identify potential hacking attempts/breaches?
- How do they stay up to date with current issues?
- Do you rely on an external IT person or company? How do you know they’ve got the right controls in place to protect you?
- Is your website secure? How do you know?
- How much customer information do you store? Do you need to keep it all?

This should be part of your regular conversation

Reducing your risk

Business continuity and incident response

- Have a plan – what would you do if you couldn't access your network? How long could you operate without it?
- Regularly back up all data and check status
- Keep copies offline – ransomware can also affect your online backups
- Test, test and retest

Thank you!

As details continue to emerge, updates and downloadable resources are available on Grant Thornton's **COVID-19 Hub**

https://www.grantthornton.ca/finding-the-way-forward-guiding-businesses-through-coronavirus

Subscribe to receive these and other updates
https://www.grantthornton.ca/Subscriptions/Subscribe/

Questions, contact:

Leah White, Partner, Advisory Services

E Leah.White@ca.gt.com