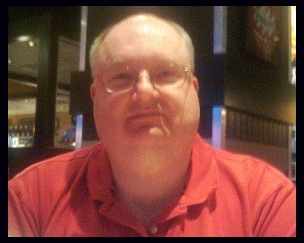
Phishing and Ransomware Attacks – They Are Coming For You! (RCSD)

Scott Quimby



January 29, 2019

The new reality – You are actively being targeted

- **Through sophisticated use of machine learning and artificial intelligence (AI), cybercriminals are actively targeting you:**
  - IT technical professionals – They have the keys to the network.
  - Financial staff – They have access to the money
  - Personnel, Guidance and Faculty – They have access to the Personal Identifiable Information (PII).
    - SchoolTool, NutriKids, Info-Matic, etc.

You are being actively targeted

- **Cybercriminals are identifying you - *by name* - to target their attacks.**
- **Attacks come in the following manner:**
  - By email (i.e. Phishing attacks)
    - Malicious attachments such as Word, Excel, and PDF files
    - Malicious web links.
  - By visiting infected web sites:
    - Malicious links
    - Clicking on invisible buttons to grant access
    - Exploiting workstation weaknesses
      - Java
      - Flash
      - Windows
  - Inserting infected USB devices into computers

The problem is very real

- **103 identity thefts per 100,000 complaints in NYS in 2019!**
- **NYS ranked 4th nationally in cybercrime in 2019**
  - Source: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
- **In 2016 Education ranked #1 in targets with 23% of the attacks.**
  - Source: https://www.sedarasecurity.com/top-3-cyberthreats-to-school-districts/

Targeted District Office/Business Office Attacks

- I have personally witnessed a banking trojan attack across the river that actively targeted the district's business office and district office. Furthermore, it specifically targeted users and machines that had access to financial data. The intensity in which it attacked those users and machines was relentless.
- Reading advanced endpoint protection logs I have seen the endless fake/infected invoices and infected documents being sent almost exclusively to another district office and business office. The cybercriminals are attempting to get a foothold on the inside of the network to launch a financial attack.

End users are the weakest link

- **True story:**
  - Local non-profit.
  - An employee working in the finance office received and email entitled, “Help I am trapped in Afghanistan!” with an attachment.
  - The finance department employee tried to open the attachment and couldn’t open it.
  - The employee got their co-worker to help open the attachment and click on it.
  - The entire finance network was compromised with a ransomware attack.
  - The tech director said they were given the data recovery bill to the two employees to pay!

Local Town

- **True story:**
  - Town Comptroller “Googled” for bank’s sign on information vs. using bookmarks of verified web links.
  - Machine was infected by Zeus trojan from on of these sites.
  - Machine captured banking sign on information and sent it to Russian Mafia.
  - Russian Mafia executed $400,000 in wire transfers from town accounts to Ukraine. Someone walked into the bank in Ukraine and walked out with the cash.

Google Docs Phishing

- **True story:**
  - A year and a half ago many district staff were sent an email with a Google Doc requesting sign on information.
  - The document was fake.
  - Entering the information in fact authorized access to these cyber criminals into the account of the person typing their information into the Google Doc.
  - A lot of districts had staff type in their contact information.
  - Thankfully:
    - It appears that this was a proof of concept attack vs. an actual attempt to steal anyone's data.

Multiple Districts

- **District payroll clerk receives a request to change direct deposit to a new account.**
  - One payroll clerk processes the request without confirmation. The first time anyone knows anything is wrong is when the employee realizes the money isn't in their account.
  - Another payroll clerk in another district confirms (not through email) that the employee in fact asked for the change and immediately discovers that it is an attempt to steal money from the district.

Multiple Districts

- **Personally identifiable information (PII) is improperly secured:**
  - One district had all the Superintendent's confidential files and all the Special Education confidential files in full view to anyone in the district (probably for years)!
  - One district had put confidential business office, payroll, and personnel files under a generic common folder and messed up the rights allowing all that information to be visible to anyone on the network.
  - One district had a vendor mis-configure rights to a district office server allowing all high school students direct access to an extremely confidential PII student share for 3 months before it was discovered.

Other notable examples

- **Miami students sue the school district for releasing personally identifiable information!**
  - https://www.miamiherald.com/news/local/education/article157361084.html
- **Montana schools held hostage and release personal student data:**
  - https://nakedsecurity.sophos.com/2019/09/21/hackers-holds-entire-school-district-to-ransom/
- **$500,000 theft from NY school district:**
  - https://krebsonsecurity.com/2010/01/fbi-investigating-theft-of-500000-from-ny-school-district/
- **$200,000 cyber theft on 9/27/18 at Galloway Township, NJ schools due to staff logon credential theft.**
  - https://www.pressofatlanticcity.com/education/missing-in-galloway-schools-cybersecurity-incident/article_0e7ca40a-34cb-5c44-a5d6-1b16088dfca1.html

Other notable examples

- **Cape Cod Community College President John Cox disclosed the cyber attack and digital theft in an email to staff and faculty on December 7, according to multiple reports. Working with banking officials, the West Barnstable, Massachusetts college has recovered about $300,000 of the funds as of Sunday, December 9, 2018 the reports say.**
  - https://www.msspalert.com/cybersecurity-breaches-and-attacks/phishing/hackers-steal-800000-from-college/
- **Officials said the hacker made off with the personal information of over 500,000 student and staff. Phishing attack**
  - https://www.zdnet.com/article/hacker-steals-10-years-worth-of-data-from-san-diego-school-district/
  - https://mashable.com/article/san-diego-school-district-data-breach/

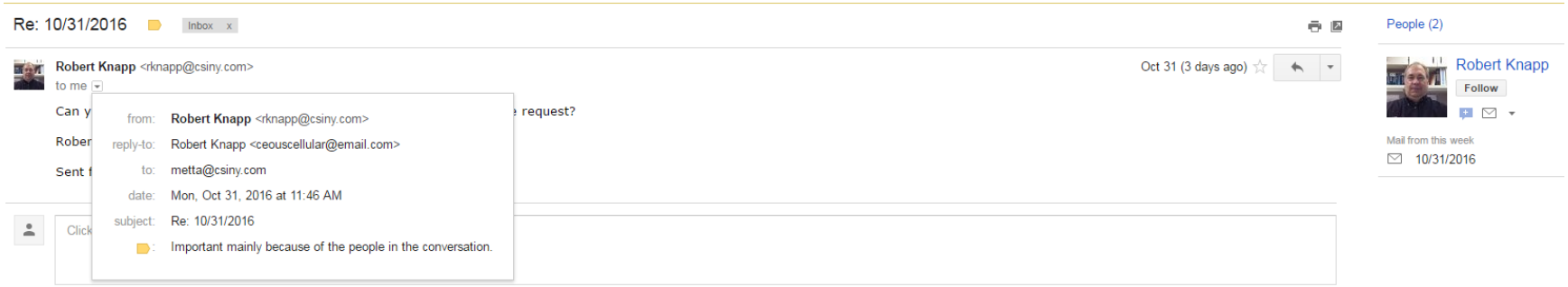
Fake Invoices

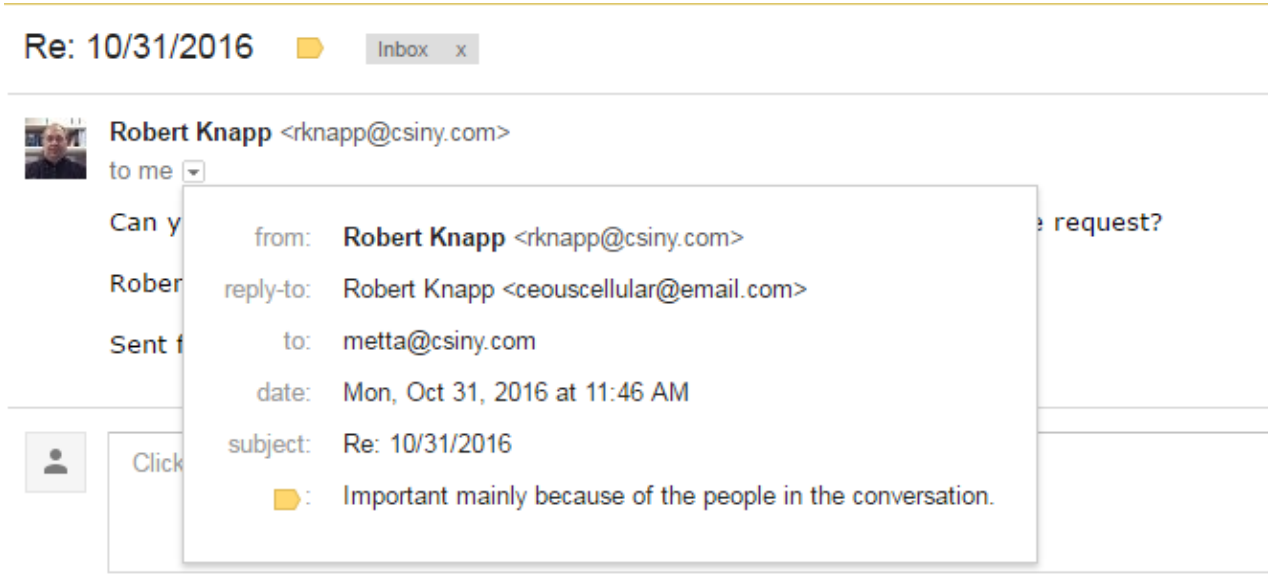
- **Lake Ridge Schools loses suit to recover $120,000 missing after hacking incident 11/25/2018**
  - https://www.nwitimes.com/news/local/crime-and-courts/lake-ridge-schools-loses-suit-to-recover-missing-after-hacking/article_8d38b9b9-6bb9-50e0-bf90-900361b4f499.html

CSI's Own Office

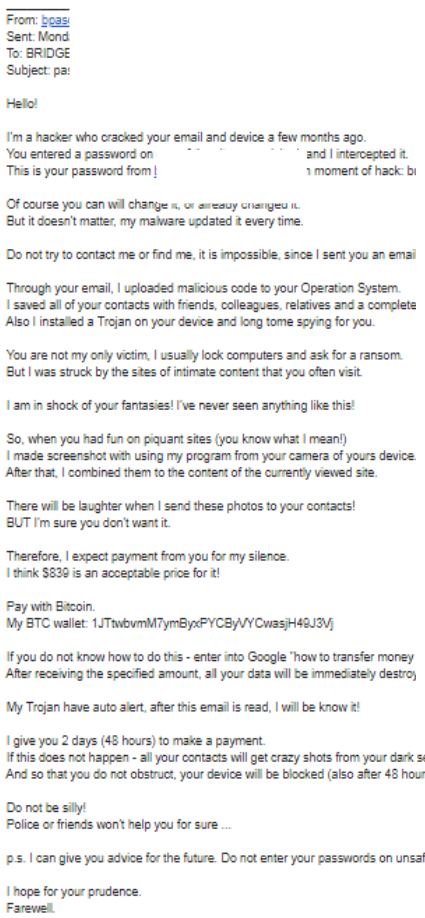
- **MaryLynn is the "money" person.**
- **"Bob Knapp" sends MaryLynn an innocent email, "Hey are you in the office?" On casual glance:**
  - It looks like it is coming from Bob's email address
  - Bob's actual Google Apps picture in on the email
- **MaryLynn is busy doing other things and replies, "yes".**
- **She gets another email, "Can you do something for me?"**
- **She replies, "sure".**
- **She gets another email, "I need you to make a wire transfer.."**
- **MaryLynn stops and realizes something is very wrong.**

The actual email





An attack going on right now in schools



From: bpas
Sent: Mond
To: BRIDGE
Subject: pas

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on and I intercepted it.
This is your password from ! moment of hack: b

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an emai

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $839 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1JTwbvmM7ymByxPYCByVYCwasjH49J3Vj

If you do not know how to do this - enter into Google "how to transfer money
After receiving the specified amount, all your data will be immediately destroy

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.

From:
Sent: Monday, October 22, 2018 10:18 PM
To:
Subject: password (bucky106) for is compromised

Hello!

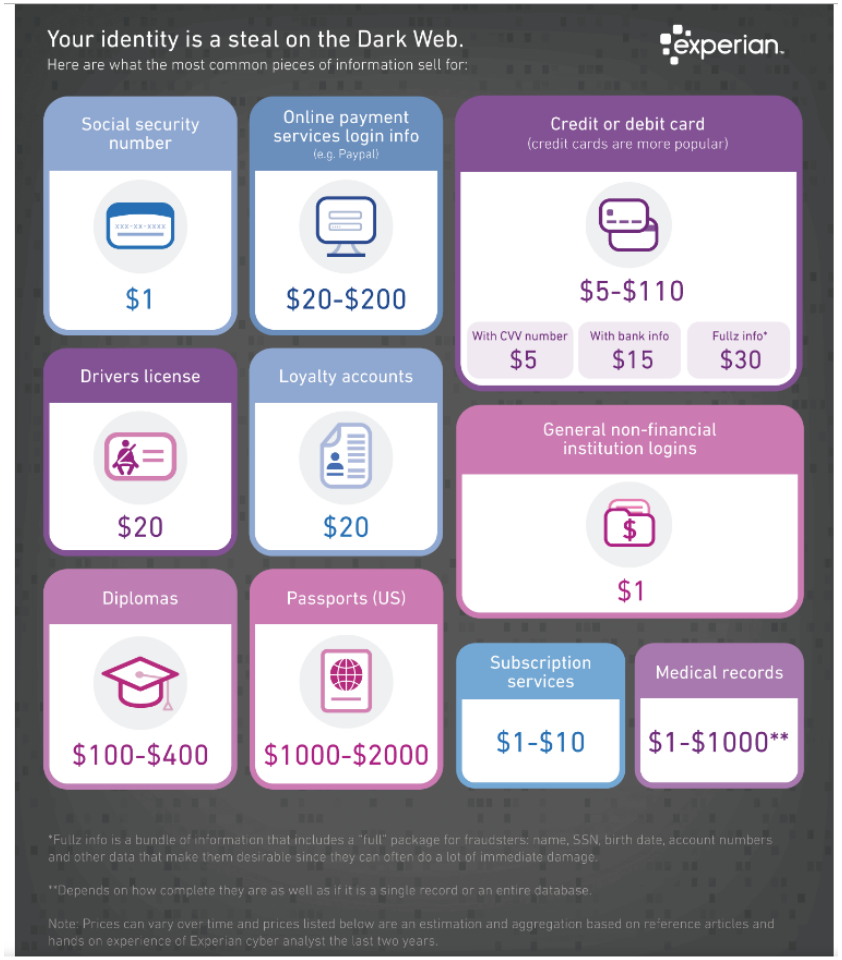
I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from on moment of hack: bucky106

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

What is going on?

- The end user's information was previously compromised.
- It is available on the "dark web".
- Cybercriminals saw sign on information and passwords previously used in the stolen information.
- They sent an email to the address they saw using a password they found as "proof" they had hacked the current user's account.
- The user's in question they we talked to had re-used their school email sign on elsewhere on other systems including re-using the same password!
- They got very scared when they saw their own information presented to them.

Your personally identifiable data is worth a lot!



What you can do

- **See something. Say something.**
  - If you see what looks like confidential information visible where it shouldn't be, immediately report this to your IT staff.
- **Faculty and Food Service have access to personally identifiable information.**
  - Logout
  - There is a reason you are asked to change your password
  - There is a reason we have password protected screen savers
  - Do not leave SchoolTool logged in when you are not there.

Web sites

- Don’t “Google” for websites containing sensitive data (i.e. financial and personal data).
- Instead bookmark the sites you use.
- The reason is that DNS (the phone book of the internet) can be poisoned and fake websites looking like your real web site are given to you.
- They capture your information and steal whatever they can.

Don’t click on suspect emails

- Spammers insert “beacons” into graphics embedded into emails.
- These beacons “phone home” to tell the spammers that your email is an valid address that they can target.

What can you do about this?

- **Save attachments before opening them.**
  - This allows the local antivirus to take one more, independent look at whether something bad is going on before you open it and potentially infect your machine.
  - Do not run any attachment that is an executable.
  - Remember that Microsoft Office macros often are used for bad purposes. If you don't need them, they can be turned off by your technology staff.
  - Remember that PDFs are an extremely popular way of infecting machines.

Is it real?

- **Trust, but verify**
  - If you are asked to do something with personally identifiable information or a monetary transaction, validate the request – not via email.
    - It is not uncommon to either get an email from real people you know making weird requests.
    - It is not uncommon to get an email from an email address which is similar enough to a real address that it fakes you out.
  - Use the phone
  - Speak to the person face to face.
- **Validate web links**
  - If you look at the entire web URL, does it really go where you think it goes?

Establish Procedures

- Establish a district wide list of, “we will never ask you via email” questions and educate staff.
- Do not re-use passwords.
- Do not cache passwords.
- Establish standards for “syncing” web browsers.
- Educate staff at home to be careful mixing school and personal web browsing on family computers.

Establish Procedures

- **Use only district approved file share systems and only with approved files.**
- **Do not click on attachments from unknown senders without understanding what is being sent to you.**
- **If you get a phishing email, stop and do not delete the email until explicitly told to do so by your technology staff.**
  - The reason is that only the original email contains the true source of the email.
  - Your technology staff may be able to block the source address to prevent others from getting similar requests.

Use Only Secure Software

- **Windows 7 and higher (not Windows XP or Vista)**
  - Apply security updates
- **Current antivirus**
- **Current versions of software**
  - Apply security updates

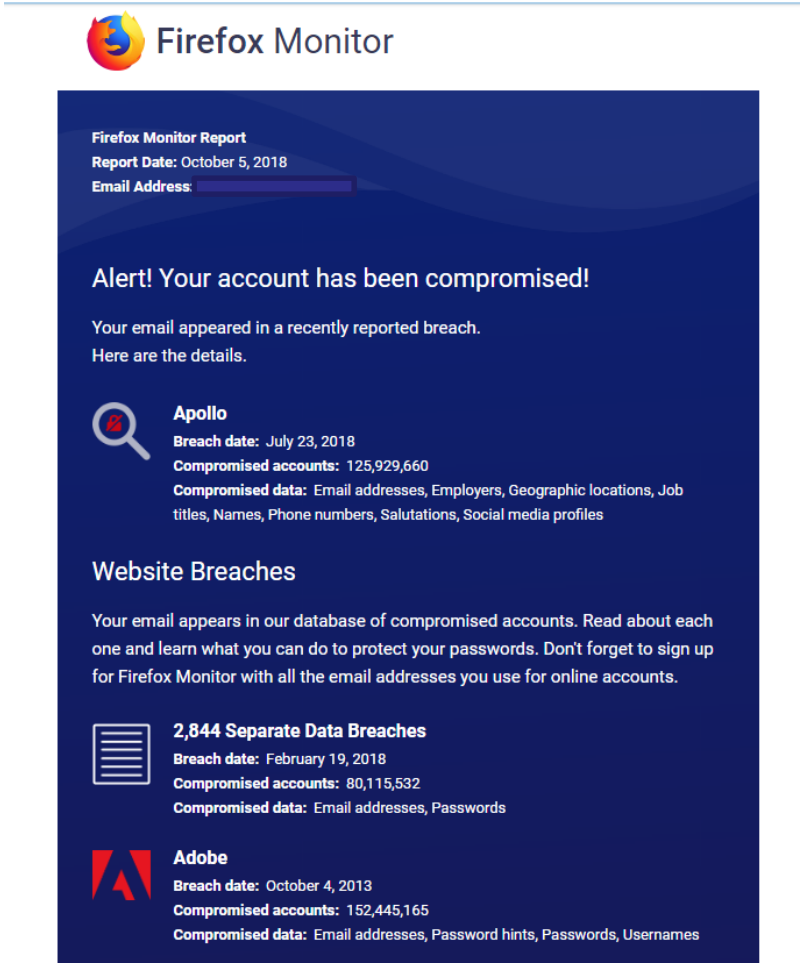
Use Multi-Factor Authentication Whenever Possible

- **Multi-Factor Authentication (MFA) means that you rely on something beyond just your logon ID and password. This could be:**
  - Texting your cellphone
  - Calling your cellphone
  - An authenticator application like Google or Microsoft Authenticator.
  - A USB stick that gives you single use codes
  - Having your cell phone near your computer
  - Your face
  - Your fingerprint

Multi-Factor Authentication

- Whenever possible turn on MFA.
- The reason is that even if someone “cracks” your password, they still can’t get into the system as you.
- Google Apps allows users to have MFA
- Microsoft Windows 10 allows users to have MFA
- Other applications and web pages do as well.
- Most MFA is free.

Firefox Monitor



Questions?

csiny.com