Phishing, CEO Fraud & Other Criminal Tactics

February 19th, 2020
Matthew Ellis, Incident Management, UBC Cybersecurity
FACTS

• At UBC, we are responsible for substantial amounts of personal information about students, faculty, staff, alumni, and donors.

• Protecting this information is everyone's responsibility.

• UBC’s highest likelihood of information security risks stem from the poor practices and lack of knowledge from end-users.
HOW VALUABLE IS UBC TO CRIMINALS?

Criminal Objective: Monetize UBC

Criminal Strategy: Find a weak link then exploit it any way you can

What you don’t know: It’s the same attacker looking at the target group as prey – if they recognize that a specific user responds to an attack then they will continue to be targeted

What you can do: Think before you respond! Report suspicious incidents to security@ubc.ca
COMMON ATTACKS TARGETING UBC STAFF & FACULTY

• CEO Fraud
• Business Email Compromise (BEC) / Social Engineering
• Invoice Malware
• Invoice Fraud
• Salary Changes
CEO FRAUD

• **Criminal Objective:** Make money from UBC via simple social engineering

• **Criminal Strategy:** Convince UBC administrative employee that their Head of unit requires an immediate activity be done. E.g. wire transfer or gift card (iTunes, Steam, Amazon)

• **What you don’t know:** They are spoofing the Head’s identity, the email isn’t really coming from the head

• **What you can do:** Talk with your head of unit and develop a strategy for validating urgent activities (I will confirm by voice, text me, call me on my cell, etc.)  !!!**Do this TODAY!!!**

LETS’S SEE SOME SAMPLES!
CEO FRAUD

1. Wed 19/09/2018 3:03 PM
   To: [email]
   Are you available?

2. > On Sep 19, 2018, at 11:06 PM, [email] wrote:
   > I'm available - in the office.
   >
--- Original Message ---
From: [redacted]
Sent: Wednesday, September 19, 2018 3:09 PM
To: [redacted]
Subject: Re: yes,

I'm in a meeting right now and that's why I'm contacting you through here. I should have called you, but phone is not allowed to be used during the meeting. I don't know when the meeting will be rounding up, and I want you to help me out on something very important right away.

---

On Sep 19, 2018, at 11:10 PM, [redacted] wrote:

No problem, if that's something I am capable. But I finish work @4:15pm
-----Original Message-----
From: [redacted]@gmail.com
Sent: Wednesday, September 19, 2018 3:15 PM
To: [redacted]@ubc.ca
Subject: Re: yes,

i need you to help me get an iTunes gifts card from the store, i will reimburse you back when i get to the office.

On Sep 19, 2018, at 11:15 PM, [redacted]@ubc.ca wrote:

No problem. Where to get? And how much. I can walk now.
CEO FRAUD

>> -----Original Message-----
>> From: [email]
>> Sent: Wednesday, September 19, 2018 3:18 PM
>> To: [email]
>> Subject: Re: yes,
>>
>> Oh good thanks The amount i want is $100 each in two (3) piece so that will make it a total of $300 I'll be reimbursing back to you. I need physical cards which you are going to get from the store. When you get them, just scratch it and take a picture of them and attach it to the email then send it to me here ok Can you get it?
>>
>> Sent from my iPhone

>> On Sep 19, 2018, at 11:21 PM, [email] wrote
>>
>> UBC Bookstore has it. I'm on my way now.
CEO FRAUD

> -----Original Message-----
> From: [redacted]@gmail.com
> Sent: Wednesday, September 19, 2018 3:23 PM
> To: [redacted]@ubc.ca
> Subject: Re: yes,
> 
> Ok if they do go get it and scratch it to send make sure it has the price on it
> 
> Sent from my iPhone
> 
>
From: <Dean of Faculty>
Date: Tuesday, March 21, 2017 at 10:30 AM
To: <recipient's email address removed>
Subject: Request

I'm in a meeting at the moment and I need you to assist in processing a payment to a vendor for a consulting service for $20,850. Can I send the details?
From: <Associate Dean of Faculty>
Sent: Thursday, April 20, 2017 7:43 AM
To: <recipient’s email address removed>
Subject: Request

Good morning <recipient’s first name>, are you in office? Please confirm you received my previous message.

Thanks,
<Associate Dean’s first name>

Sent from my iPhone
Hello,
I will need your assistance to get me some gift cards for a presentation for the teenagers program I'm invited to speak. Get back to me when you are available.

Ps, I'm occupied at the moment can't take calls right now email me back.

Thanks
Lindi Frost
Hi Jean-Paul,

Are you available, I need you to process a wire transfer.

Regards,

Santa
CEO FRAUD

Sample #6a of 6

Sat 09/02/2019 10:56 PM

Santa J Ono
<santaj_ono@my.com>

Urgent!

Are you currently available?

Santa J Ono
santaj_ono@my.com
University of British Columbia
CEO FRAUD

Sample #6b of 6

From: Santa J Ono
To: MECH Reception

Urgent!
February 9, 2019 at 10:55 PM

Are you currently available?

Santa J Ono
santaj_ono@my.com
University of British Columbia
BEC: SOCIAL ENGINEERING

Criminal Objective: Make money from UBC via complex social engineering (man-in-the-middle)

Criminal Strategy: Convince UBC finance employee that the email is via an existing genuine vendor/UBC relationship

What you don’t know: The company is real but the email address belongs to the criminal organization

What you can do: Carefully check email addresses – look for slightly different domains. E.g. matthew.ellis@mail-ubc.com - check for differences to addresses/banking details
BUSINESS EMAIL COMPROMISE

Criminal emails Widgets.com pretending from UBC and orders a $75K in widgets products to be shipped to a UBC “remote” site – provides a PO

Widgets ships the product and invoices UBC

UBC receives the invoice but cannot reconcile the order and requests a copy of the order from Widgets

Criminal sells the widgets products and makes easy money!!

Who is the victim???
Mon 24/09/2018 10:38 AM
Dennis Silva <dennissilva-ubc@outlook.com>

QUOTE REQUEST

To: Dennis Silva

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

Attention: Courriel Externe

I would like to check product availability and price quotation for the items below:

3 units ..... Cisco WS-C3850-12X48U-L 48 10/100/1000 UPOE Ethernet ports Switch

3 units ..... Cisco 4451-X Integrated Services Router

200 unit...... Seagate Seagate 1TB Backup Plus Slim External Hard Drive USB 3.0 2.5" 4 Colors Portable Hard Drive HDD For Desktop And Laptop

Let me have the unit cost of the item(s) if in stock. Do advise the pricing and availability of the items.
Purchasing/Payment Terms: Our Institution standard Payment terms is Net 10 or Net 30 from the date of your Invoice. Awaiting your earliest response

Regards
Dennis Silva
Director, Payment & Procurement
The University Of British Columbia
2329 West Mall, Vancouver BC V6T 1Z4
BUSINESS EMAIL COMPROMISE – HOW DOES THIS WORK?

The Set-up

- Criminal intercepts email via compromised account at either UBC or the vendor (Widgets Construction)
- Criminal identifies vendor relationship between Jane @ UBC (jane.smith@ubc.ca) and John @ Widgets (john.hancock@widgets.com)
- Criminal sets up two domains: ubcc.ca and widgetts.com then creates email accounts (jane.smith@ubcc.ca and john.hancock@widgetts.com)
BUSINESS EMAIL COMPROMISE

The Switcheroo

• Criminal emails Jane @ UBC from the *fake* john.hancock@widgetts.com and requests a change of banking information for future payments
• Jane asks John to confirm company details before she can update the payment details
• Criminal emails John @ Widgets from the *fake* jane.smith@ubcc.ca and reports there’s a new process at UBC and needs additional details for future invoices (John provides details)
• Criminal emails Jane @ UBC from the *fake* address with the details provided by John
• Jane changes the payment details
BUSINESS EMAIL COMPROMISE

The Score

• Criminal waits – maybe months for an actual invoice to be sent from Widgets

• UBC pays the criminal – possibly multiple times!!!
INVOICE MALWARE

Criminal Objective: Make money from UBC via ransomware

Criminal Strategy: Entice UBC finance employee to open a file by convincing them it’s a statement or invoice

What you don’t know: The file is actually malicious and will encrypt all of their files

What you can do: Be vigilant! Often the email will contain a password because the criminals had to encrypt the file in order to get it pass antivirus scanners. If the attachment was really confidential then would they have put the password in the email? That makes no sense!
INVOICE MALWARE

From: Baudru, Jamie Lee
To: security.administrator@ubc.ca
Cc: 
Subject: FW: the statement from Riley Hancock [UNSCANNED] [UNSCANNED]

Message:

-----Original Message-----
From: Riley Hancock [mailto:h.gehrke@t-online.de]
Sent: February 15, 2017 7:54 AM
To: AUDI ML Clinical <sass-clinical@audiospeech.ubc.ca>
Subject: the statement from Riley Hancock [UNSCANNED]

Good morning
Review the statement attached.

You may need Doc Access Credentials: BTvkfp

Kindest regards
Riley Hancock
INVOICE FRAUD

Criminal Objective: Make money from UBC via social engineering

Criminal Strategy: Convince UBC finance employee that an invoice is unpaid and outstanding

What you don’t know: The invoice is a fake

What you can do: Review invoice handling procedures – check that the supporting documentation aligns with the invoice
INVOICE FRAUD

No passcode/password = no virus
SALARY CHANGE TO PAY/SCHEDULE FOR STEALING CREDENTIALS OR MALWARE DEPLOYMENT

**Criminal Objective:** Steal credentials or infect computer(s) with malware.

**Criminal Strategy:** Entice UBC employee to open a file or login to a website by convincing them there’s a change to their salary or payment schedule.

**What you don’t know:** Employees worry about their paycheque and the criminals use that to scare you into doing what they want.

**What you can do:** Understand UBC polices. UBC doesn’t do this.
HELPDESK <vwebb2@atu.edu>

Important Notification Regarding 2017 Payroll.

Dear Member,

You have 1 new Important security notification regarding 2017 payroll schedule.

View Message Now.

Best Regards,
The University Of British Columbia.
SALARY CHANGE TO PAY/SCHEDULE

http://patrickrummans.com/www/webmail.alumni.ubc.ca
ANOTHER THING...DOES TIMING MATTER?

- **Yes** – fiscal year end is a good time to attack because you’re busy rushing around
- We see surges at fiscal year end and the start of session
THIS SOUNDS DREADFUL...WHAT CAN YOU DO?

- Be vigilant!
- Bookmark the Privacy Matters website privacymatters.ubc.ca
- Take the Privacy & Information Security - Fundamentals training 1 & 2
- Encourage your team and co-workers to take the training
- Encrypt your mobile devices if you haven’t already
- Learn how to report an information security incident or potential privacy breach
WHAT CAN WE DO?

• Understand that you are never wasting our time!
• When something looks unusual contact security@ubc.ca – the malicious message might be widespread and the earlier it is reported the better!
• Cybersecurity is here to help
• But what if it’s a false-positive and we waste of your time?
  • No such thing: Cybersecurity would rather spend time looking at a few “safe” messages than miss the “malicious” ones and have to deal with the cleanup from those
  • Cleanup from incidents is far more impactful than reviewing a safe message!
• Focus on Privacy Matters is available to assist you in improving privacy and information security practices in your area. Visit privacymatters.ubc.ca/focuson or contact privacy.matters@ubc.ca for more information on how to get started.
Questions or Comments?