



Don't Be Phooled by the Phish

Educating Staff about the Dangers of Phishing

Joanna Cook

East Noble School Corporation
Director of Technology

jcook@eastnoble.net
@enmediagirl



Josh Walters

East Noble School Corporation
1:1 Manager, Lead Technician,
Network Assistant

jwalters@eastnoble.net
@jwalters310

To Access Our Presentation:

<https://delivr.com/2g2u8>

To Access Our YouTube Videos:

<https://delivr.com/2du44>

WHO ARE WE?

- PreK-12 Public School District in northeastern Indiana
- Eight schools—5 elementary, 1 middle, 1 high school, 1 Alternative Learning Center
- 3,700 Students
- Finishing 8th year of being 1:1 in grades K-12





WHY THE FOCUS ON CYBERSECURITY?

Two Reasons:

- INDOE Cybersecurity Initiative
- BrightBytes Data indicated need



INDOE Cybersecurity Initiative

- Indiana felt need to bring multi-faceted focus on Cybersecurity across the state—students, teachers, and districts
- Cybersecurity for Staff
 - 86 districts piloted MediaPro as a phishing platform for the 2018-2019 school year.
 - MediaPro also supplied cybersecurity training resources.
 - District had to agree to provide PD to staff regarding the dangers of phishing.



BrightBytes Data Indicated
a Need to Focus on Digital
Citizenship

- *67% of teachers spend less than 3 hours a year teaching about online safety.*

Digital Citizenship & Cybersecurity

- Realization that many teachers lacked the knowledge about digital citizenship to instruct students in these topics.
- Decided to make our focus on TEACHERS this first year.



IDOE / ENSC

CYBERSECURITY

AWARENESS



ENSC CYBERSECURITY
AWARENESS CAMPAIGN

THINK BEFORE YOU CLICK. POST. TYPE.



WHAT DOES IT TAKE?

ESTABLISH THE NEED

- STUDENTS: To make learning relevant, we need to make ***connections*** with things they already know or are familiar with.
- STAFF MEMBERS: To make learning relevant, we need to make ***connections*** with things they already know or are familiar with.

Our goal was to use as many local examples of cyber incidents as possible to create a sense of doom/urgency about cybersecurity.

Rising ED TECH Usage + Collection of Student Data = **MAJOR RISK**



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Sep 13, 2018
Alert Number
I-091318-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

EDUCATION TECHNOLOGIES: DATA COLLECTION AND UNSECURED SYSTEMS COULD POSE RISKS TO STUDENTS

The FBI is encouraging public awareness of cyber threat concerns related to K-12 students. The US school systems' rapid growth of education technologies (EdTech) and widespread collection of student data could have privacy and safety implications if compromised or exploited.

EdTech can provide services for adaptive, personalized learning experiences, and unique opportunities for student collaboration. Additionally, administrative platforms for tracking academics, disciplinary issues, student information systems, and classroom management programs, are commonly served through EdTech services.

As a result, types of data that are collected can include, but are not limited to:

- personally identifiable information (PII);
- biometric data;
- academic progress;
- behavioral, disciplinary, and medical information;
- Web browsing history;
- students' geolocation;
- IP addresses used by students; and
- classroom activities.

MAJOR IMPLICATIONS

If this data is compromised, cyber criminals can use it to:

- THREATEN STUDENTS—Reports of stolen data being used to threaten parents, publicize private information, and help child predators identify new targets.
- THREATEN EMPLOYEES—If employee data is leaked, cybercriminals could use private data to file tax returns and receive refunds, redirect payroll deposits, etc.

“Learn these skills to keep YOUR personal data safe. Learn these skills to keep OUR STUDENTS’ personal data safe!”

3 BASICS ELEMENTS OF THE ENSC CYBERSECURITY INITIATIVE

1. Phishing Campaign

- Email “Campaigns” sent throughout the year.
- Anyone that clicked on phishing links saw this screen
- Three Strikes and You’re OUT—IDOE/ENSC Cybersecurity Course assigned



That’s a phishing scam, and you took the bait!

Cyber criminals use compelling e-mail messages—such as this one—designed to trick you into clicking a link or downloading an attachment. Once you’ve taken the bait, they steal sensitive information or install malicious software on your computer.

You should have deleted this message or moved it into your spam folder without clicking on the link.

2. Professional Development for Staff



IDOE/ENSC Cybersecurity Basics Preventing Phishing



Introduction

If you or anyone you know has ever been hooked by phishing, you know it's more than just an annoyance that fills our inbox. In fact, it's a criminal activity that defrauds individuals and ruins companies, costing billions of dollars each year.

Put simply: phishing is the most significant risk to our information.

You are the target of this cybercrime—but you're also our best chance at avoiding this risk. If you develop the right attitude and the right skills, you can keep us—and yourself—safe from cybercrime.

 To learn more, click **OBJECTIVES**. When you are finished, click **NEXT**.

 **OBJECTIVES**

Name:

Password:



3. ENSC Cybersecurity Awareness Emails

- Branded every email with these words in the subject line
- Inform staff of current scams going on; any important security events would have “ENSC Cybersecurity Alert” in its place.
- Asked people to take a moment to read and watch attached videos
- PURPOSE? Breakdown the basic skills about spotting phishing

ENSC Cybersecurity Awareness: Hacked: Not IF, but WHEN--Why NOT to use Public Wifi

Joanna Cook
To: All Staff

Reply Reply All Forward ...
Wed 4/17/2019 3:57 PM



Connecting to public or free Wi-Fi access points...every single one of us have done it at some point in time.

And while nearly all of us can say that we know it's probably not the safest method to use to be on the internet, that generally does not stop us from connecting when we feel the itch to access our email, respond to a post on social media, or make a quick bank transfer. It seems that most people feel that way; at the 2016 Democratic and Republican Conventions, nearly 70% of the attendees connected to the non-secure Wi-Fi at both conferences (<https://hbr.org/2017/05/why-you-really-need-to-stop-using-public-wi-fi>). If the registered delegates of these conventions think it's ok to do it, it should be fine, right?? You couldn't be any more WRONG!

Connecting to public Wi-Fi can be compared to driving without a seatbelt; not taking the recommended precautions can have long-lasting, harmful effects. While you might be ok driving in a car without a seatbelt sometimes, should you choose not to put it on and get in an accident, it could have very bad consequences. *Every time you log on to free Wi-Fi in a store, a coffee shop, a hotel, or an airport, it's like rolling the dice.* It's not a question of if you will be hacked...it's a question of WHEN you will be hacked.

Public Wi-Fi can be hacked in a large number of ways, and it doesn't take someone with a Master's Degree in Computer Science to figure out how. In fact, there are hundreds of YouTube videos that show people how to do just that. According to my research, there are two main ways to access your personal data from public Wi-Fi. The first way is called "Man in the Middle." With this technique, internet traffic is intercepted between your device and the destination by making your device think the hacker's machine is the access point to the internet. The other way is called "Evil Twin." Many hackers will create access points using the Wi-Fi Hot Spots on their phones or laptops and name them something almost identical to the verified network of the place you are at. Thinking you are joining a legitimate network, you innocently connect to the hacker's network where **everything** you do can be monitored.

THE IMPORTANT PART—HOW TO PROTECT YOURSELF REGARDING FREE WIFI:

- NEVER use public Wi-Fi to do online shopping, access PowerSchool, log into your bank, or to go to any service or website that holds sensitive information. EVER.
- Turn OFF the feature on your cell phone that automatically logs you into Wi-Fi so that it doesn't seek out and join Wi-Fi without your knowledge.
- Turn OFF your Bluetooth connection on your cell phone or laptop to ensure that others are not able to intercept your data that way.
- Sign up for an unlimited data plan for your devices and stop using public Wi-Fi altogether, if possible.
- KEEP YOUR MACHINE up to date with the latest security updates so there are no software vulnerabilities for a hacker to exploit. This includes operating system updates and manufacturer updates.
- Always keep a firewall running on your device so that it is more difficult for someone to access your device through the network (here at East Noble, all devices are protected by the Fortinet Firewall).
- Make sure your devices have good anti-virus/anti-malware software on them. (Again, here at East Noble, this is done through the Forti-Client installed on all machines.) However, make sure any personal devices you own also have some kind of protection running on them. You can install Forti-client on home devices for free at www.forticlient.com.
- Turn your computer OFF if you are not using it when you are in public places where you would be more vulnerable to this type of incident.
- If you have access to a VPN (virtual private network), always use that as a means to access secure sites over public Wi-Fi.

To fully understand how EASY it is for hackers to steal your usernames, password, and data on public Wi-Fi, PLEASE take a moment to watch at least one of the following videos based on your time and desire to learn. You will gain a healthy level of suspicion every time you travel and will not spontaneously join a public Wi-Fi without thinking about what you are doing—I can guarantee it!

PUBLIC WI-FI: A GATEWAY FOR HACKERS—This 2 ½ minute video by CNN Business gives you a quick glimpse into how easily a hacker is able to create a Wi-Fi network in an airport and monitor the information being sent over that network



How Did We Start?

Summer Phishing Campaign

- Used to establish a baseline of where staff knowledge was and to become familiar with MediaPro.

The screenshot shows a web interface for configuring a campaign. It has tabs for 'Details', 'Targets', and 'Logs'. The 'Details' tab is active, showing fields for Name, Description, and Schedule. The 'Targets' tab is also visible, showing a list of email templates.

Callout 1: Name of Campaign. I always included what week it was so that I could easily identify when a campaign ran. (Points to the Name field: 2019.End of Year #3--Card Services)

Callout 2: Staff names and email addresses are listed here. (Points to the Targets tab)

Callout 3: Campaign start and end dates are set here. (Points to the Start and Stop sending e-mails on date pickers)

Callout 4: Email templates were chosen here. (Points to the 'Card Services--2019 End of Year' entry in the E-mail Templates list)

Form Fields:

- Name: 2019.End of Year #3--Card Services
- Description: (Empty)
- Schedule:
 - Start sending e-mails on: 04/15/2019 04:00 PM
 - Stop sending e-mails on: 04/28/2019 11:59 PM
 - Turn off links on: 04/28/2019 11:59 PM
- Landing Page:
 - Force a single Landing Page:
 - Outstanding Expense Report Landing Page
- E-mail Templates:
 - Buttons: Add Templates, Remove Checked, Remove All
 - Show: 10 entries
 - Search: (Empty)
 - Table:

NAME	ACTIONS
Card Services--2019 End of Year	<input type="checkbox"/>
 - Showing 1 to 1 of 1 entries
 - Navigation: Previous 1 Next



Sat 5/19/2018 3:16 PM

receipt@appl.com

Your receipt from Apps.

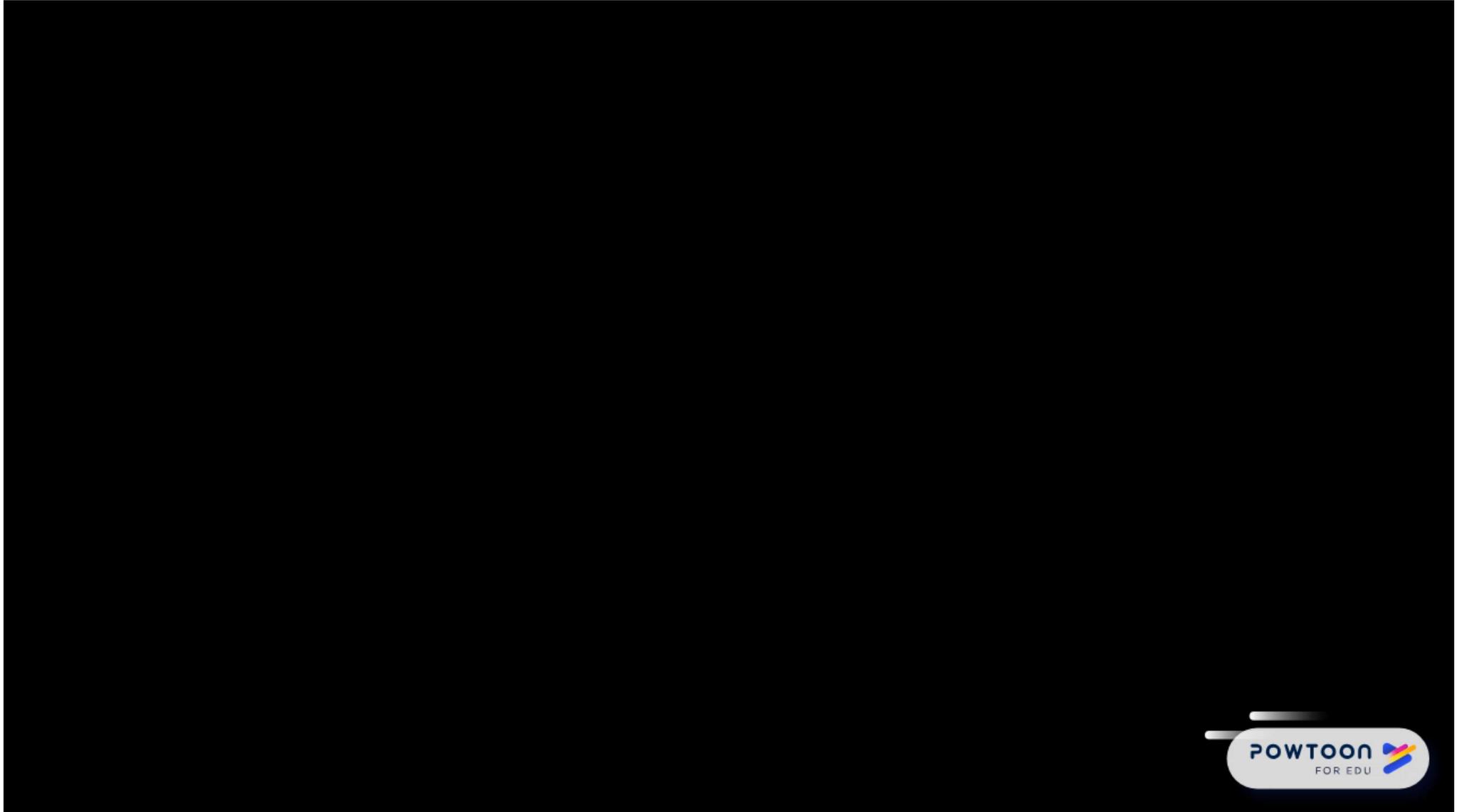
To Joanna Cook



APP STORE	TYPE	PURCHASED FROM	PRICE
Mobile Legends: Bang bang, 1,000 Diamonds Report a problem	In-App Purchase	iPhone 7 Plus	\$19.99
		Total	\$19.99
		Tax	\$0.00

22% of our staff members clicked the link!
(103 staff members total)

First Teacher Day—*Build the Anticipation*



Week #1

- Launched 3 Phishing emails

From: tracking@expressdelivery.com
To: targets@contoso.ltd
Date: Thu, 25 Apr 2019 12:46:33 -0400
Subject: A Package is Headed Your Way

Dear Customer,

Thank you for choosing Express Delivery for your shipment. This is to confirm that one or more items in your order have been shipped.

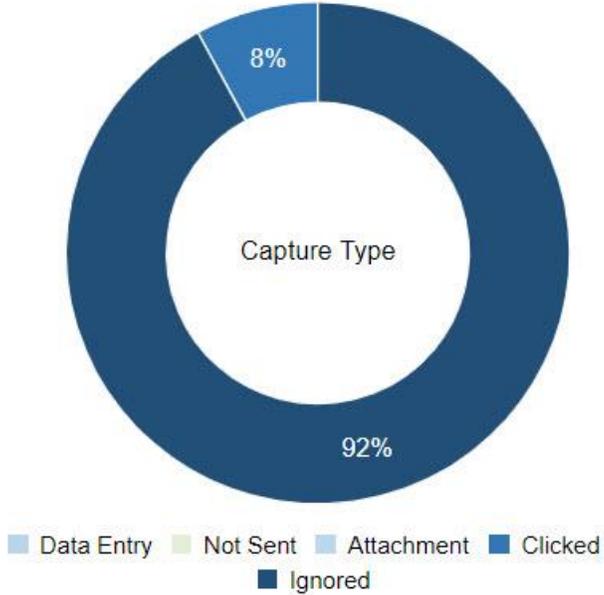
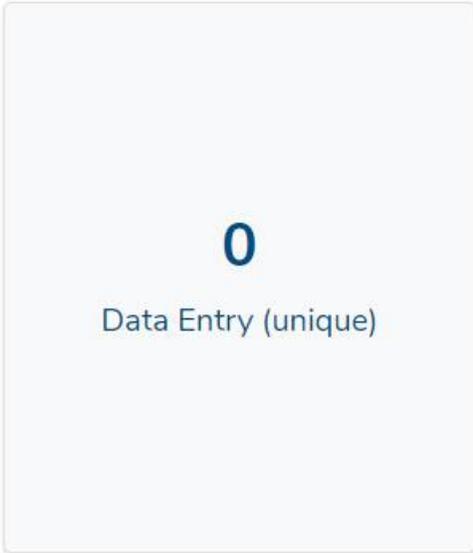
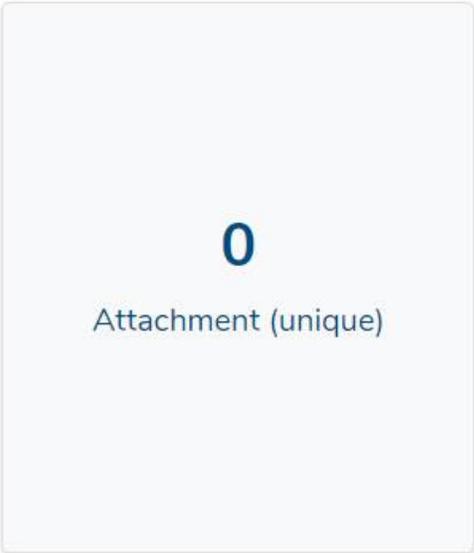
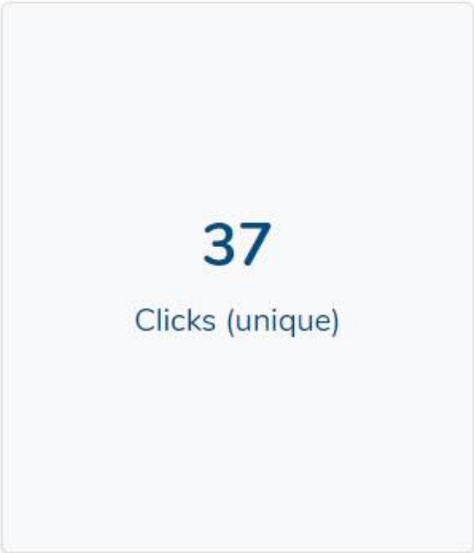
To track your package, click this link:

<http://www.expressdelivery.com/URDknvckafd24a>

Sincerely,
The Express Delivery team

How did we do?

Week #1--Express Delivery



Tip: Share Results with Staff so they are Vested in the Process



Email Follow-ups Breaking Down What to Look for to Determine if a Message is Phishing

ENSC CYBERSECURITY AWARENESS: Ways to Catch a Phish--Part 1

Joanna Cook
To All Staff

Reply Reply All Forward

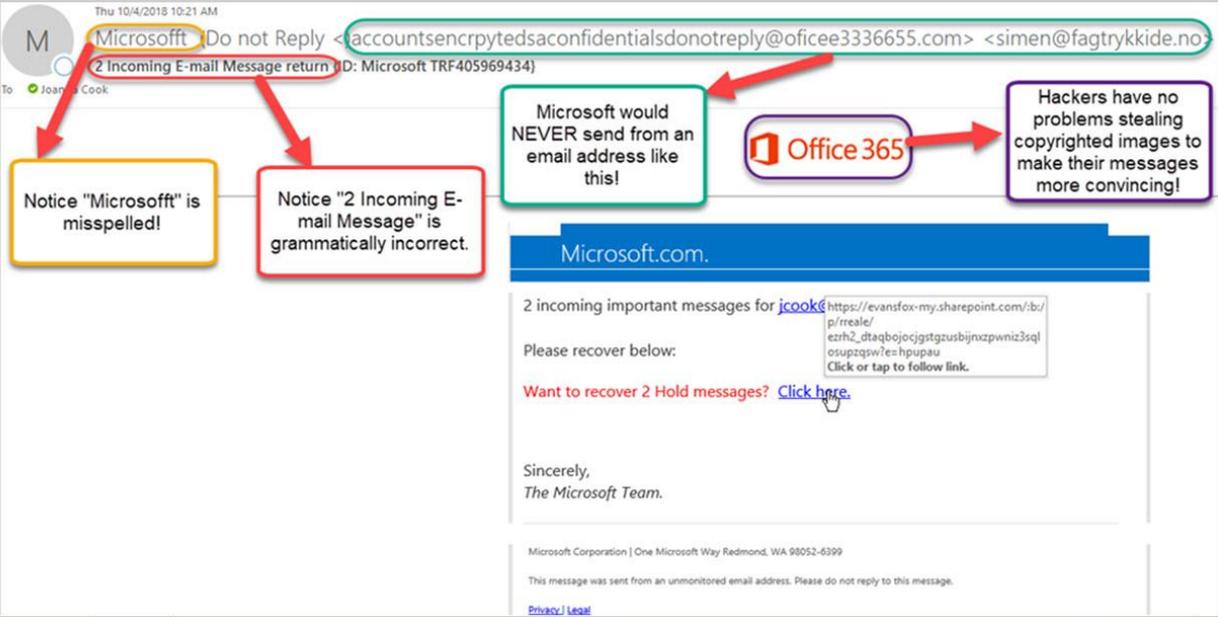
Tue 10/23/2018 7:48 AM

The examples in these emails have come straight out of my own inbox and are either ones I have received or ones people have forwarded to me. These attacks happen DAILY! Here's step one in what to look for to spot phishing emails!

WAYS TO CATCH A "PHISH"—Part 1

CHECK THE SENDER!

- The most important step in identifying a phishy email is to identify the sender. If you don't know them, you should IMMEDIATELY be on guard.
- And even if you do...take a moment to really LOOK at the "From" address, and keep the following in mind:
 - Scammers use NAMES and EMAILS stolen on the black market, so their messages appear to be from real people.
 - An extremely common tactic is to spoof a well-known service's address, like your email provider or bank.
 - Hackers aren't always great at grammar and spelling! Check to make sure the sender's name is spelled correctly. (Notice in this email Microsoft is spelled with two "tt's".)
 - If something seems off, compare the senders email address to the real service's email address—a difference in even ONE LETTER should set off an alarm!



The screenshot shows an email from "Microsoft" with a subject line "Do not Reply" and a sender address that is a long, complex string of characters. Annotations highlight several red flags:

- Notice "Microsofft" is misspelled!** (The sender name is misspelled with two 't's).
- Notice "2 Incoming E-mail Message" is grammatically incorrect.** (The subject line contains a grammatical error).
- Microsoft would NEVER send from an email address like this!** (The sender address is suspiciously long and complex).
- Office 365** (The sender address contains the Office 365 logo).
- Hackers have no problems stealing copyrighted images to make their messages more convincing!** (The Office 365 logo is a copyrighted image).

The email body contains a link to a SharePoint site and a request to recover messages. The footer includes the Microsoft Corporation address and a disclaimer.

ENSC CYBERSECURITY AWARENESS: Tip #2--Check That Link Carefully!

Joanna Cook
To: All Staff

Reply Reply All Forward ...
Wed 10/24/2018 11:25 AM

WAYS TO CATCH A "PHISH"—Part 2



CHECK THAT LINK CAREFULLY!

- THE MOST IMPORTANT THING you can do to avoid falling prey to phishing is to check any hyperlink's URL BEFORE clicking! In other words...DON'T CLICK UNTIL YOU HOVER!
- If you hover over the hyperlink in any email by moving the cursor on top of the link, a popup will appear that gives the TRUE location of where the link will take you.
- If that link doesn't match the sender, IT'S A FAKE!
- Remember...JUST ONE CLICK by one person on a phishing link endangers the whole network.
- Again...DON'T CLICK UNTIL YOU HOVER!

Thu 10/4/2018 10:21 AM
Microsoft (Do not Reply <accountsencrytedsaconfidentialsdonotreply@office3336655.com> <simen@fagtrykkide.no>
2 Incoming E-mail Message return (ID: Microsoft TRF405969434)
To: Joanna Cook

This link is definitely NOT coming from Microsoft! Sometimes it's very obvious...like this one. But sometimes it's off by just a few letters. Read these links carefully!

Microsoft.com

2 incoming important messages from jcool

Please recover help

Want to recover 2 Hold

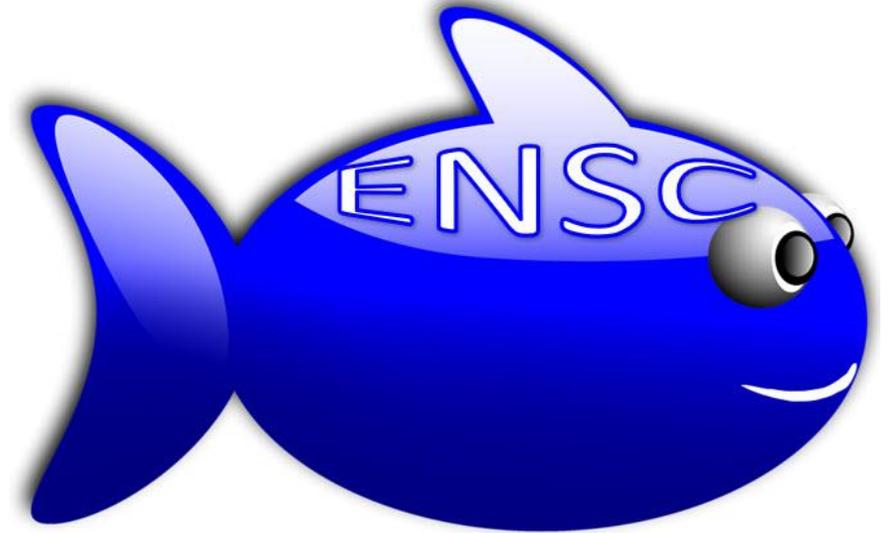
Sincerely,
The Microsoft Team.

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-0337
This message was sent from an unmonitored email address. Please do not reply to this message.
Privacy / Legal

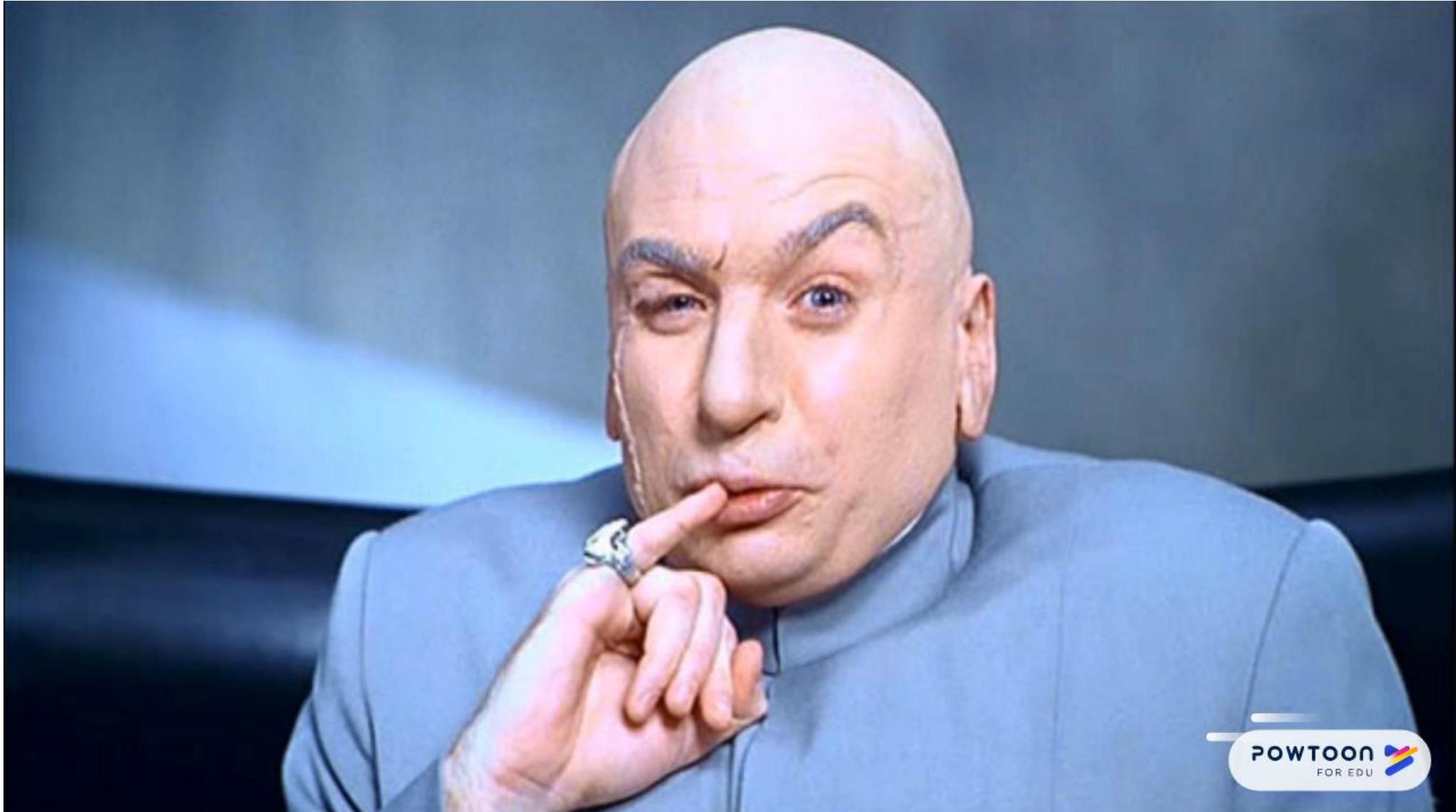
https://evansfox-my.sharepoint.com/:b/d/p/rreal/ezrh2_dtqbojocjstgzusbijnxzpniz3sqlosupzqsw?e=hpupau
Click or tap to follow link.
Click here.

“Catch a Phish” Basic Skills Covered Over the Next Few Weeks

1. Check the sender
2. Check all links carefully.
3. Beware of attachments.
4. Don't be fooled by fake sign-in pages.
5. Check the Eng-lish.....
6. Beware of alarmist messages insisting you act immediately.



Dr. Evil Shared Three Week Results



Other Topics Covered—Holiday Dangers

ENSC CYBERSECURITY AWARENESS: 'Tis the Season...FOR PHISHING! BE ON ALERT!

Joanna Cook
To: All Staff

Reply Reply All Forward
Mon 11/19/2018 9:16 AM



As the holiday season approaches and many of us get wrapped up in the “buying phrenzy” of Black Friday, Cyber Monday, and everything else, please know that phishing scams will be on the rise. In just the last week, I have received notices from Huntington Bank and Professional Federal to be on the lookout for common phishing scams, so know that major organizations are on high alert during this time. If you think that in 2017, *over 3.4 BILLION dollars was spent on Cyber Monday alone*, it makes sense that cyber crimes increase during the months of November and December. Additionally **FRAUD INCIDENTS JUMP 50% OVER THE AVERAGE IN THE MONTHS OF OCTOBER, NOVEMBER, AND DECEMBER!**

Brian Leitch received this notice from a member of the Association of School Business Officials International that he is a member of warning of an Amazon scheme they have seen going around lately. Be on the lookout for the following:



Nov 12, 2018 1:47 PM
Karen Smith

There is a new type of phishing email scam just in time for the holidays!

The phishing email is from a vendor such as Amazon thanking the individual for their order and showing what the individual ordered. It is typically something an individual would not order such as 10 routers. The email indicates if you did not place the order, click on the order number. Once you click on the order number, it asks for your login and password.

With the holiday shopping season approaching, it is a good time to remind employees, family and friends of these type of phishing email scams and to be suspicious of these type of emails.

Karen Smith CPA RTSBA CIA
Asst Supt Business & Financial Svcs
Cypress-Fairbanks ISD
karen.smith1@cfisd.net
Houston, TX
United States

Take one minute and watch the following video for a brief reminder about what to look out for! You've done an amazing job at thinking about what you are clicking on from the beginning of the campaign until now.



Remember to THINK before you CLICK. POST. And TYPE this holiday season! Have a great Thanksgiving, everyone!

Cyber-extortion

ENSC CYBERSECURITY AWARENESS: Cyber-extortion emails circulating in the district



Joanna Cook
To All Staff

Reply Reply All Forward ...

Mon 12/3/2018 1:26 PM



WARNING; some of the content in this email may be disturbing to some of you...but that's the point of sharing it. You see, this email is an example of a growing trend that is gaining traction online now, and that is something that is called *cyber-extortion*. Cyber-extortion is when someone online threatens some sort of harm to you unless you meet their demands. Generally this demand is in the form of money (in the example below, you will see they ask for bitcoins, which is common), but the extortionist could demand basically anything.

Just last week, several people around the district, along with myself, received the below email. The subject line on the email was this: "jcook@eastnoble.net was hacked! Change password immediately!"

Hello!

I have very bad news for you.

03/08/2018 - on this day I hacked your OS and got full access to your account jcook@eastnoble.net On this day your account jcook@eastnoble.net has password: xxxxxxx

So, you can change the password, yes.. But my malware intercepts it every time.

How I made it:

In the software of the router, through which you went online, was a vulnerability.

I just hacked this router and placed my malicious code on it.

When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.

But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!

I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea...

I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).

After that, I made a screenshot of your joys (using the camera of your device) and glued them together.

Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.

I think \$776 is a very, very small amount for my silence.

Besides, I have been spying on you for so long, having spent a lot of time!

Events in the News

ENSC CYBERSECURITY AWARENESS: San Diego School HACKED



Joanna Cook
To All Staff

Reply Reply All Forward

Thu 1/3/2019 1:30 F



THIS IS WHY WE ARE DOING THIS...

THIS IS WHY we keep sending emails and “fake phishing” your accounts.

THIS IS WHY you need to read and watch the information about cybersecurity being sent.

THIS is the headline of an article in Newsweek today:



As cybercriminals get more and more sophisticated, we are going to continue to be barraged with more and more attempts to steal our student and employee information. Although it's hard to tell from this article exactly how this particular instance occurred, it does point to phishing as a possible source of the intrusion. JUST ONE CLICK on a link or responding to an unknown person's request for usernames and passwords can lead to drastic damage to our network and information.

Spear Phishing

ENSC CYBERSECURITY AWARENESS: They are watching YOU...SPEAR PHISHING!

Joanna Cook
To: All Staff

Reply Reply All Forward
Mon 1/21/2019 2:48 PM



The majority of you now have a pretty good eye for catching phishing emails when they arrive in your inboxes. You have learned to look for spelling errors, hover over links in emails to see where the true destination of the link is going to, to never click on attachments you are not expecting, and to always think before you click, post, or type. Now that you can spot these attempts, you might shake your head when you receive one and wonder how someone would ever fall for something like this (which someone on my staff just received):

-----Original Message-----
From: mrs joan williams <info@admin.com>
Sent: Friday, January 18, 2019 3:27 PM
Subject: PLEASE CONFIRMED IF YOU ARE ALIVE

ATTENTION,

THIS SERVES AS MY FINAL MAIL AS I HAVE CONTACTED YOU BEFORE WITHOUT RESPONSE FROM YOU, IT IS ABOUT YOUR (\$5MILLION) WE WERE MANDATED TO TRANSFER TO YOU, BUT WE NEED TO CONFIRM FROM YOU IF YOU ARE ALIVE.

Looks ridiculous, right? While emails like this may have seemed worrisome to you before you started learning about phishing, hopefully now you know to simply click DELETE on your keyboard and move on to the next email. However, what if I told you that cybercriminals are specifically watching YOU? Would you believe it? You should, because phishing is becoming more and more sophisticated. Another type of phishing is called SPEAR PHISHING. **Spear phishing emails are emails that are TARGETED at a SPECIFIC individual or a SPECIFIC ORGANIZATION that appears to come from a TRUSTED source.** These are PERSONALIZED MESSAGES meant JUST FOR YOU. Spear phishing attackers try to get as much

ENSC CYBERSECURITY AWARENESS: They are watching YOU...SPEAR PHISHING!

Joanna Cook
To: All Staff

Reply Reply All Forward
Mon 1/21/2019 2:48 PM

Networking sites such as Facebook and LinkedIn might have your email address, who your friends are, your geographic location, and any posts about recent purchases or trips they can find. They then use this information to act as a familiar friend or business and send a convincing but very fraudulent message to you, the target.

WHAT CAN YOU DO TO AVOID A SPEAR PHISHING ATTACK?

1. Watch what personal information you are posting on the internet. Look at your online profiles and see how much of your personal information is available for attackers to view. If there is anything you don't want a potential scammer to see, take it off your profile...or at the very least make sure you adjust your privacy settings to limit what people can see.
2. Have smart passwords and don't use just one password for every account that you own. If a hacker can break your password in one place and you use it for multiple accounts, he or she will soon have access to all of the accounts you use it for!
3. Update, update, update! When you are notified updates are available, do them as soon as possible. Software creators constantly push out updates to defend against current attacks.
4. Don't click on links in emails! If an organization sends you a link, instead of clicking on the link, go directly to the site by typing the link in the browser instead of clicking.
5. Use your head! If something seems phishy, it probably is. Simply DELETE!

Watch the following brief video for a better idea of what spear phishing is. One note...the last slide of this says always report phishing emails to IT. We ask that you simply DELETE emails instead of reporting them as there is not much we can do about these types of email getting through when they do.



And remember...always THINK before you CLICK. POST. TYPE.

Spoofting

ENSC CYBERSECURITY AWARENESS: SOPHISTICATED PHISHING HAPPENING NOW



Joanna Cook
To All Staff

This message was sent with High importance.

Reply Reply All Forward

Wed 2/13/2019 2:25 PM

While all of these emails about cybersecurity may have been driving some of you crazy, THIS is the reason we keep discussing it. ENSC has had at least 10 employees in the last hour that have had emails sent from "their" accounts to other people and students in the district. If you look at the example below and in the email Samantha Jarrett sent to her staff, you can see that while this email says it is from senders in our district, the sending email addresses are NOT legitimate email address for our district. Why is this all happening at once, you may ask? Cyber criminals locate email listings, such as the ones on our websites, and use those listings to specifically target other users into clicking links since they are probably familiar with the name of the sender. We did have a few users click some of these links without thinking simply because they saw the familiar name and reacted. JUST REMEMBER...in this day and age, we have to STUDY EVERYTHING and QUESTION things that we get before clicking on links. If you get any more of these, please delete without clicking on any links. Hopefully you are all seeing that this is a very real threat and that knowledge about these threats is KEY!

OUR EMPLOYEE

NOT OUR EMAIL ADDRESS

Wed 2/13/2019 12:09 PM
Jaime Carroll <h-20-r-4@vanilla.ocn.ne.jp>
Fw: to you
To [REDACTED]

On Wednesday, February 13, 2019 10:01 AM, Jaime wrote:
just something nice for you to check <http://ln7e.oxyiomua.host/>

SUSPICIOUS EMAIL ADDRESS

Privileged Users

It was mandatory that all users with administrative access in Powerschool take the IDOE/ENSC Cybersecurity Course. Additionally, they had PD focused on their role and why it was important for them to be aware of cybersecurity safety even more so than “normal” users.



Tip: Base Campaigns on Needs--Attachments



Send

To...

Joanna Cook;

Cc...

Bcc...

Subject

High Documents

Attached



From: membership colemca.net <membership@colemca.net>

Sent: Friday, January 25, 2019 11:33 AM

Subject: High Documents

Good Morning

Please find the documentation and computation proposal coming up this February 2019. Let me know if you would be interested in working on it with us. The PDF sent is being protected due to the new security rules of the company. To open this secure link, we'll need you to enter the email that this item was shared to.

Thanks!

Mindy Cope

Membership Director

COLE CENTER FAMILY YMCA

E: membership@colemca.net

P: 260.347.9612

F: 260.347.1915

From: Brian Bohlender <bohlender@bartoncoevilamaa.com>

Sent: Friday, January 25, 2019 7:40 AM

To: Brian Bohlender <bohlender@bartoncoevilamaa.com>

Subject: FW: Construction Project Payment Issues

Clients:

I apologize you may be receiving this twice, but we are trying to get it out ASAP.

We have learned of two recent instances of emails being sent to school business offices, from imposter emails pretending to be from general contractors on construction projects. Within the email, the imposter requests that the payment method be changed to an ACH deposit. They have also asked for follow-up information such as when the last payment was made, etc.

The emails are sophisticated and use general contractor company logos and convincing email addresses, except that the imposter emails end with “---.us” instead of “---.com”.

In at least one case, the imposter has also attempted to call the business office to discuss payments.

Please be wary of any emails and phone calls from contractors directly to your business office on these matters. In both cases, the scam was discovered by calling back the official business office number of each contractor and learning that the emails were not legitimate.

Thank you

Brian Bohlender, AIA, LEED AP, ALEP

Vice-President

Barton-Coe-Vilamaa

Architects & Engineers



TIP: You Can Build a Phishing Campaign on emails You Receive Without Sophisticated Programs

ENSC Cybersecurity ALERT: Matt Rickey Direct Deposit Incident Stopped; HIGH ALERT!

Joanna Cook
To: All Staff

This message was sent with High importance.

Reply Reply All Forward ...
Mon 4/15/2019 2:41 PM



Good afternoon, everyone. Immediately after Spring Break, we had a cybersecurity incident involving a high school teacher that was STOPPED due to the quick thinking of our HR department. However, you need to be AWARE this is happening and take as many steps as possible to avoid putting yourself at risk for this same type of incident. This has recently happened in TWO districts in our area and the school districts were unable to get the money back that was stolen using this technique!

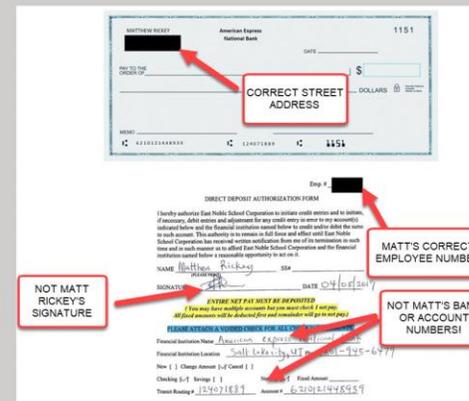
On Friday, Melissa Gibson (Human Resources Director) received an email from who she thought was Matt Rickey, East Noble High School social studies teacher. The email was an inquiry about how to change his direct deposit information. Here is the email from "Matt" to Melissa. You will notice it is coming FROM Matt's email address. However, you will notice there are some subtle grammar errors in the email. The person claiming to be Matt also sets a tone of urgency because he wanted the bank account information changed before the next pay period, which was a few days after this email.



Melissa Gibson responded by saying that in order to change the direct deposit information, "Matt" would need to bring a copy of a voided check into the superintendent's office and complete a Direct Deposit Authorization Form. Shortly after Melissa sent the form to this person, she received this email:



Along with this email, this individual attached a copy of a check WITH MATT'S HOME ADDRESS on it (I have taken this out for his privacy). Additionally, the Authorization Form was attached giving new bank account information to deposit money into. THIS FORM WAS FILLED OUT WITH MATT'S CORRECT EMPLOYEE NUMBER, which would be difficult for anyone outside of East Noble to know.



Even prior to receiving this information, Melissa had a feeling that something was "fishy" with these emails, as the emails were written in a tone and with errors that she knew Matt Rickey wouldn't have or use. She adamantly requested that "Matt" bring the forms in in person so that she could verify they were truly coming from him (AGAIN...THESE EMAILS CAME FROM HIS EMAIL ACCOUNT.) The individual became frustrated by Melissa's insistence that he bring the forms in in person and stopped contacting her. Additionally, Melissa called the high school to verify from Matt that he was not sending these emails. HAD MELISSA NOT CAUGHT THIS, MATT RICKEY'S LAST PAYROLL CHECK WOULD HAVE BEEN DEPOSITED IN THIS STRANGERS ACCOUNT AND THERE WOULDN'T HAVE BEEN MUCH WE COULD DO ABOUT IT. Melissa's quick thinking stopped this incident from happening because she followed some of the best practices we have been working on this year and listened to the voice in her head that said things seemed fishy.

HOW DID THIS INDIVIDUAL GET ACCESS TO MATT'S EMAIL ACCOUNT TO BE ABLE TO SEND THESE EMAILS? Matt did what nearly all of us have done many times in our lifetimes...HE JOINED A PUBLIC WIFI NETWORK WHILE TRAVELING IN FLORIDA OVER SPRING BREAK!! AFTER ACCESSING THE INTERNET THROUGH THIS INSECURE CONNECTION, HIS EMAIL WAS HACKED AND HIS EMAIL ADDRESS AND PASSWORD WERE USED TO ACCESS HIS EMAIL ACCOUNT, LEARN HIS EMPLOYEE NUMBER, AND SEND THESE EMAILS. How many of you have accessed public wifi in places like airports and coffee shops and then checked emails, done online banking, access social media accounts, etc? Nearly ALL OF US.

ENSC Cybersecurity Awareness: Hacked: Not IF, but WHEN--Why NOT to use Public Wifi

Reply Reply All Forward ...

Wed 4/17/2019 3:57 PM



Joanna Cook
To All Staff



Connecting to public or free Wi-Fi access points...every single one of us have done it at some point in time.

And while nearly all of us can say that we know it's probably not the safest method to use to be on the internet, that generally does not stop us from connecting when we feel the itch to access our email, respond to a post on social media, or make a quick bank transfer. It seems that most people feel that way; at the 2016 Democratic and Republican Conventions, nearly 70% of the attendees connected to the non-secure Wi-Fi at both conferences (<https://hbr.org/2017/05/why-you-really-need-to-stop-using-public-wi-fi>). If the registered delegates of these conventions think it's ok to do it, it should be fine, right?? You couldn't be any more WRONG!

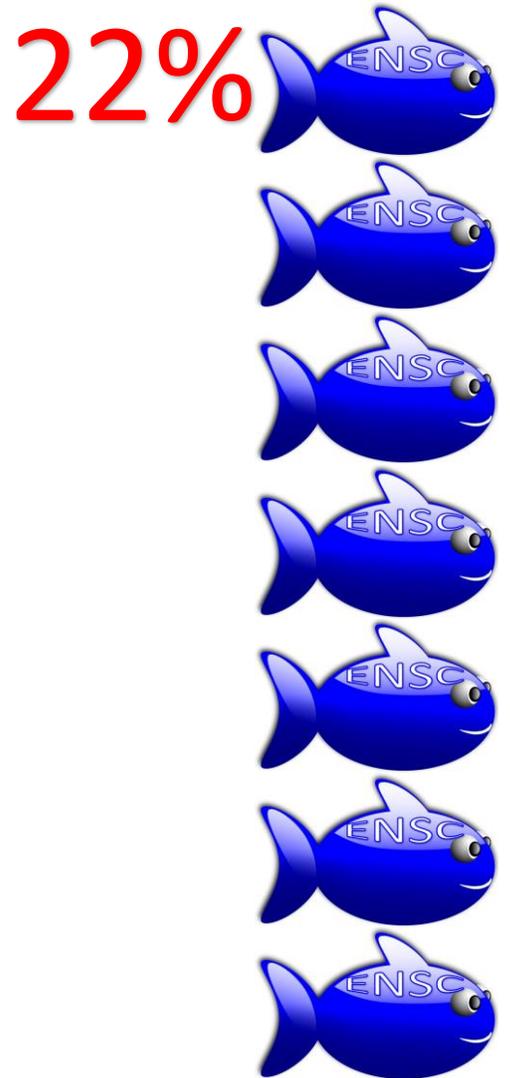
Connecting to public Wi-Fi can be compared to driving without a seatbelt; not taking the recommended precautions can have long-lasting, harmful effects. While you might be ok driving in a car without a seatbelt sometimes, should you choose not to put it on and get in an accident, it could have very bad consequences. *Every time you log on to free Wi-Fi in a store, a coffee shop, a hotel, or an airport, it's like rolling the dice.* It's not a question of IF you will be hacked...it's a question of WHEN you will be hacked.

Public Wi-Fi can be hacked in a large number of ways, and it doesn't take someone with a Master's Degree in Computer Science to figure out how. In fact, there are hundreds of YouTube videos that show people how to do just that. According to my research, there are two main ways to access your personal data from public Wi-Fi. The first way is called "Man in the Middle." With this technique, internet traffic is intercepted between your device and the destination by making your device think the hacker's machine is the access point to the internet. The other way is called "Evil Twin." Many hackers will create access points using the Wi-Fi Hot Spots on their phones or laptops and name them something almost identical to the verified network of the place you are at. Thinking you are joining a legitimate network, you innocently connect to the hacker's network where **everything** you do can be monitored.

THE IMPORTANT PART—HOW TO PROTECT YOURSELF REGARDING FREE WIFI:

- NEVER use public Wi-Fi to do online shopping, access PowerSchool, log into your bank, or to go to any service or website that holds sensitive information. EVER.
- Turn OFF the feature on your cell phone that automatically logs you into Wi-Fi so that it doesn't seek out and join Wi-Fi without your knowledge.
- Turn OFF your Bluetooth connection on your cell phone or laptop to ensure that others are not able to intercept your data that way.
- Sign up for an unlimited data plan for your devices and stop using public Wi-Fi altogether, if possible.

HAS IT WORKED?



Initial Campaign
103 People Clicked



Mid-Year
37 People Clicked



End of Year
15 People Clicked

FUTURE PLANS

- Ransomware
- USB Campaign
- Password Security
- The Internet of Things



Can't stop...WON'T STOP!

TAKEAWAYS

- It's imperative you create a sense of need—convince them of why this is important!
- While having a phishing platform is nice for data, you could base an awareness campaign off of nothing more than phishing emails you get in your corporation every day or things in the news.
- Staff members like to hear how they are doing and have appreciated learning these skills because they know it keeps them safe not only professionally, but personally as well!
- In today's day and age, this has to be an ongoing process. When we figure out the newest way people are scamming others, new ones have already launched.





**ENSC
CYBERSECURITY
AWARENESS
CAMPAIGN**

**Think Before You
Click. Post. Type.**

Joanna Cook

East Noble School Corporation
Director of Technology

jcook@eastnoble.net
@enmediagirl



Josh Walters

East Noble School Corporation
1:1 Manager, Lead Technician,
Network Assistant

jwalters@eastnoble.net
@jwalters310

To Access Our Presentation:

<https://delivr.com/2g2u8>

To Access Our YouTube Videos:

<https://delivr.com/2du44>