CT255
Introduction to Cybersecurity

Lecture 5

Human Security

- Social Engineering -

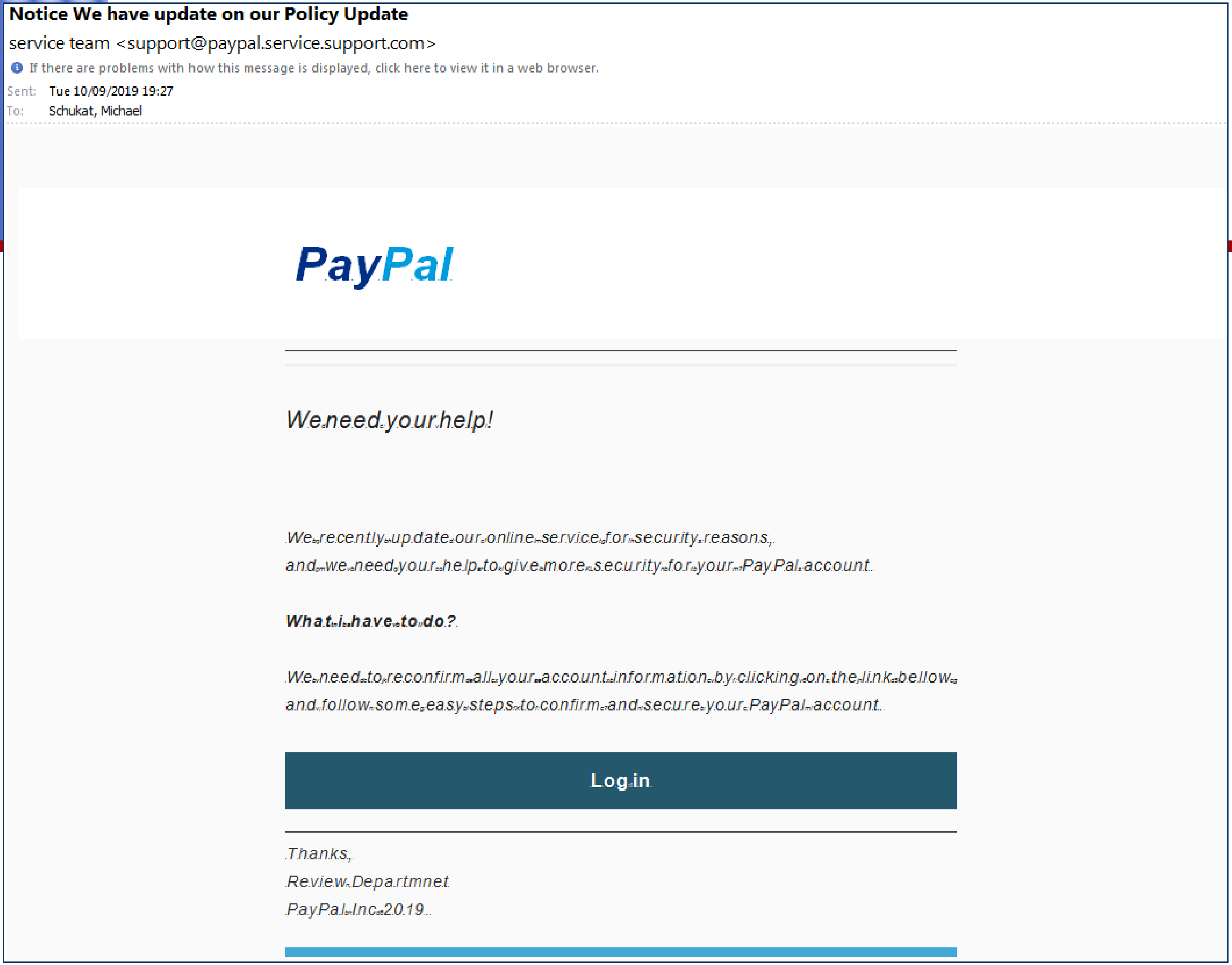
Dr. Michael Schukat, 2019-2022

Social Engineering

- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes; this includes
  - Credit card details
  - PPS number
  - Bank account details
  - Login IDs and passwords

Phishing

- Attackers use emails, social media, instant messaging and SMS to trick victims into providing sensitive information or visiting malicious URL in the attempt to compromise their systems
- Study the email on the next slide. Why is it a phishing email?



Notice We have update on our Policy Update

service team <support@paypal.service.support.com>

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

Sent: Tue 10/09/2019 19:27

To: Schukat, Michael

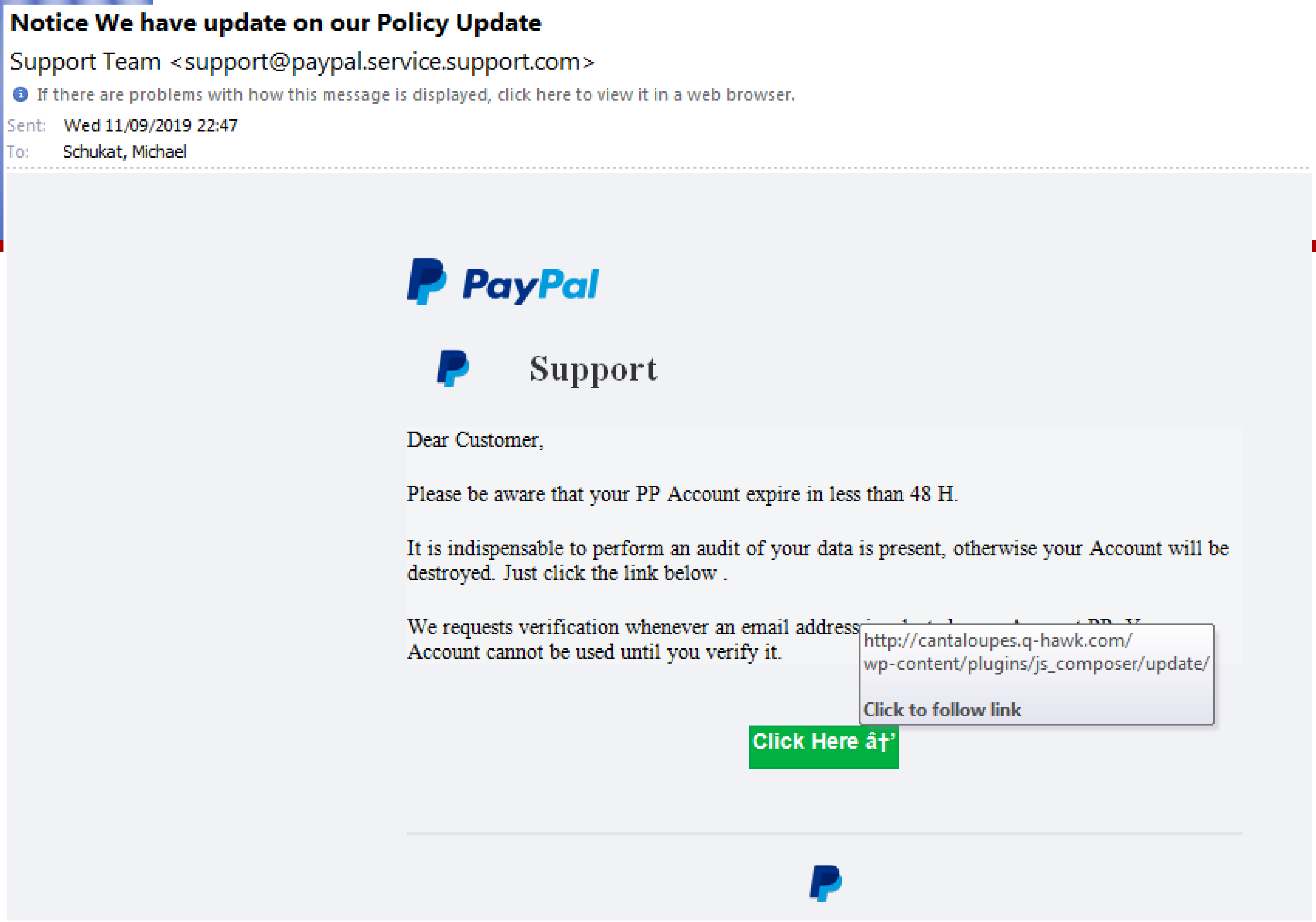
We need your help!

We recently update our online service for security reasons, and we need your help to give more security for your PayPal account.

What i have to do?

We need to reconfirm all your account information by clicking on the link bellow and follow some easy steps to confirm and secure your PayPal account.

Thanks,
Review Departmnet
PayPal Inc 2019



Notice We have update on our Policy Update

Support Team <support@paypal.service.support.com>

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

Sent: Wed 11/09/2019 22:47
To: Schukat, Michael

Dear Customer,

Please be aware that your PP Account expire in less than 48 H.

It is indispensable to perform an audit of your data is present, otherwise your Account will be destroyed. Just click the link below .

We requests verification whenever an email address
Account cannot be used until you verify it.

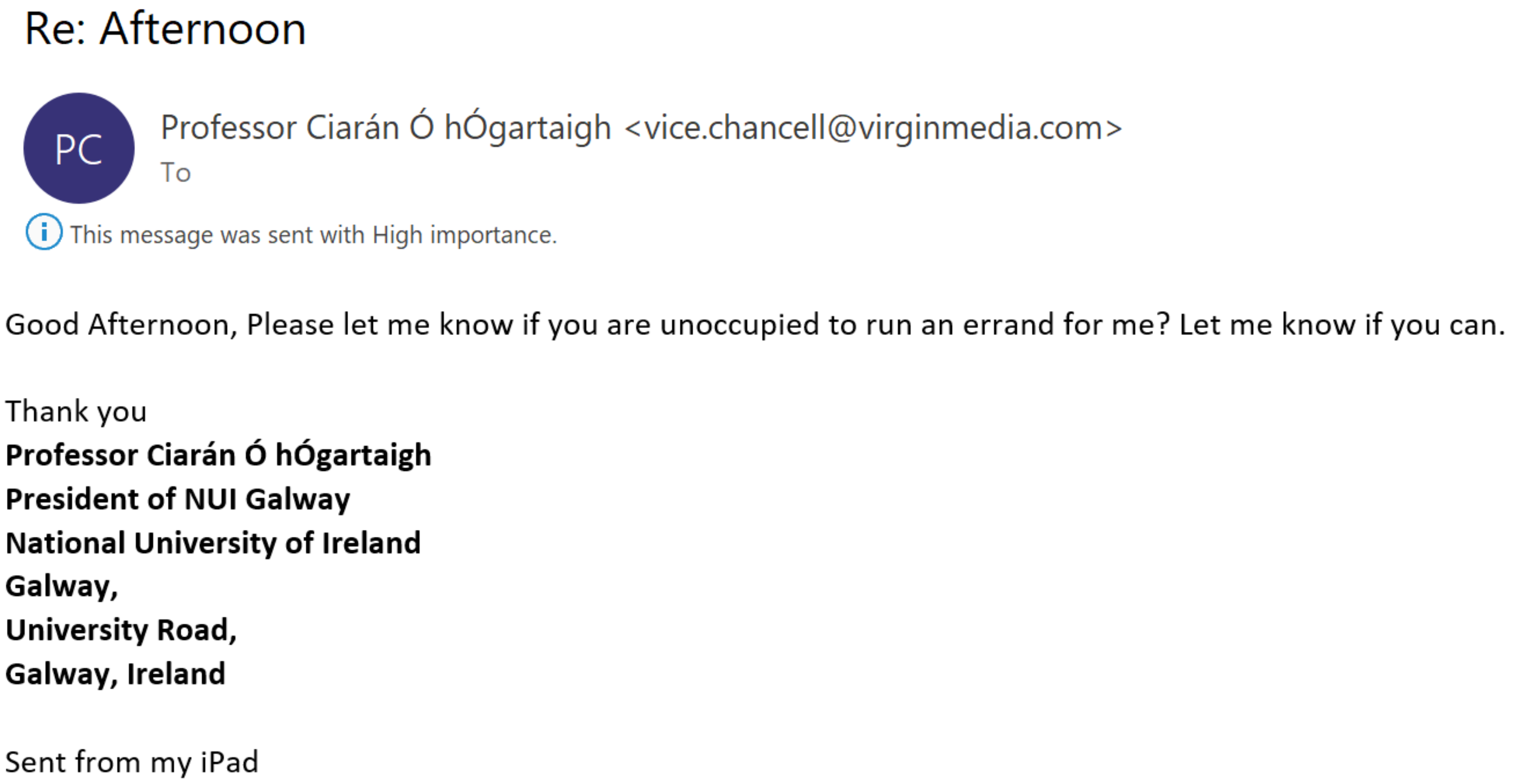
http://cantaloupes.q-hawk.com/
wp-content/plugins/js_composer/update/

Click to follow link

Spear Phishing vs. Phishing vs. Whaling Attacks

- **Phishing** involves sending malicious emails from supposed trusted sources to as many people as possible, assuming a low response rate
- In **spear phishing** the perpetrator is disguised as a trusted individual (boss, friend, spouse)
- **Whaling** uses deceptive email messages targeting high-level decision makers within an organization, such as CEOs and other executives.
  - Such individuals have access to highly valuable information, including trade secrets and passwords to administrative company accounts

Example for Spear Phishing Email



Re: Afternoon

PC

Professor Ciarán Ó hÓgartaigh <vice.chancell@virginmedia.com>

To

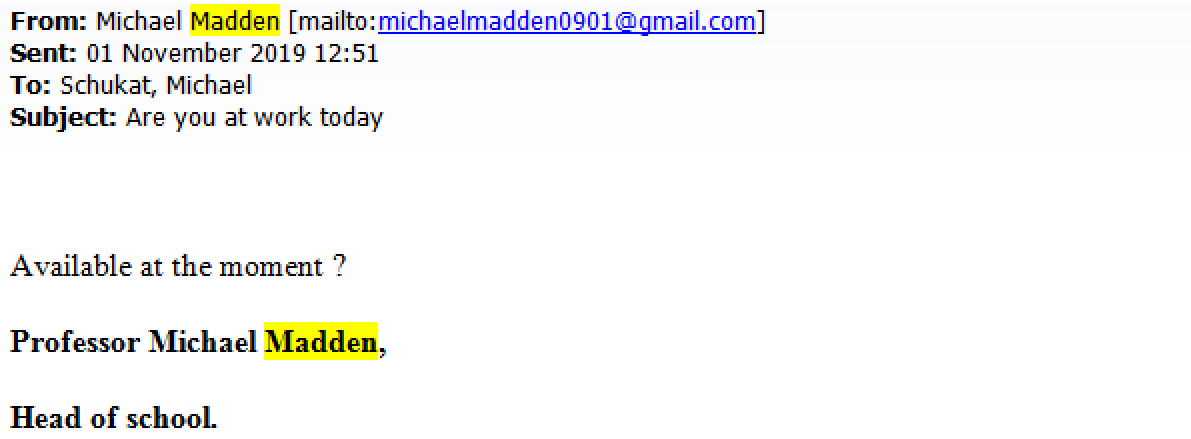
This message was sent with High importance.

Good Afternoon, Please let me know if you are unoccupied to run an errand for me? Let me know if you can.

Thank you
Professor Ciarán Ó hÓgartaigh
President of NUI Galway
National University of Ireland
Galway,
University Road,
Galway, Ireland

Sent from my iPad

Example for Spear Phishing Email Trail #1



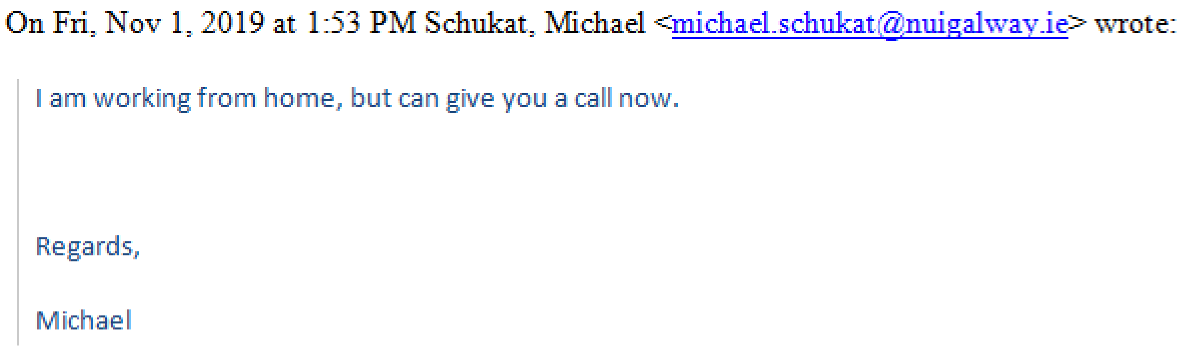
From: Michael Madden [mailto:michaelmadden0901@gmail.com]
Sent: 01 November 2019 12:51
To: Schukat, Michael
Subject: Are you at work today

Available at the moment ?

Professor Michael Madden,

Head of school.

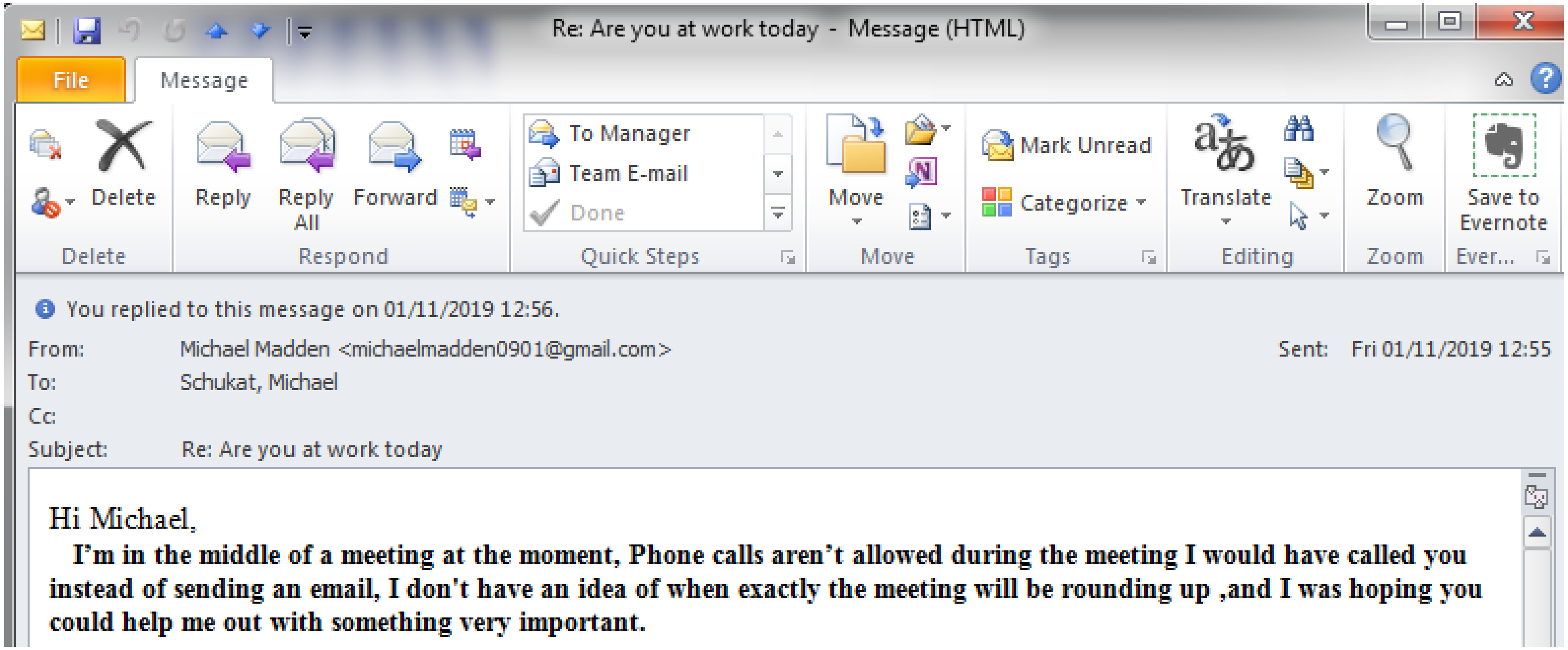
Example for Spear Phishing Email Trail #2



On Fri, Nov 1, 2019 at 1:53 PM Schukat, Michael <michael.schukat@nuigalway.ie> wrote:

> I am working from home, but can give you a call now.
>
> Regards,
>
> Michael

Example for Spear Phishing Email Trail #3



You replied to this message on 01/11/2019 12:56.

From: Michael Madden <michaelmadden0901@gmail.com>

Sent: Fri 01/11/2019 12:55

To: Schukat, Michael

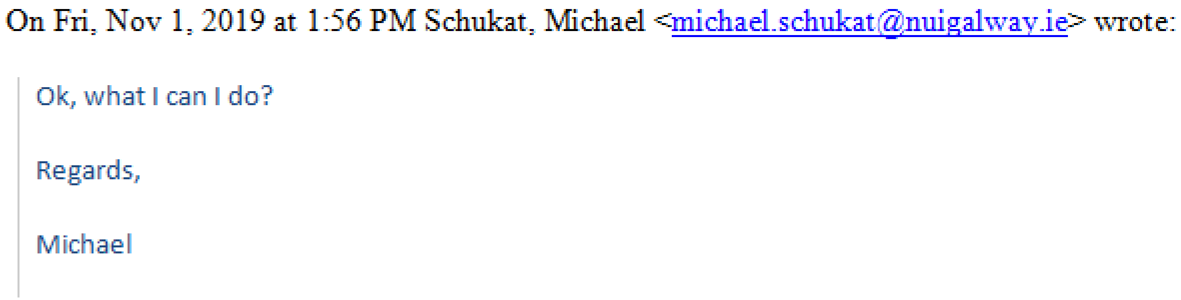
Cc:

Subject: Re: Are you at work today

Hi Michael,

I'm in the middle of a meeting at the moment, Phone calls aren't allowed during the meeting I would have called you instead of sending an email, I don't have an idea of when exactly the meeting will be rounding up ,and I was hoping you could help me out with something very important.

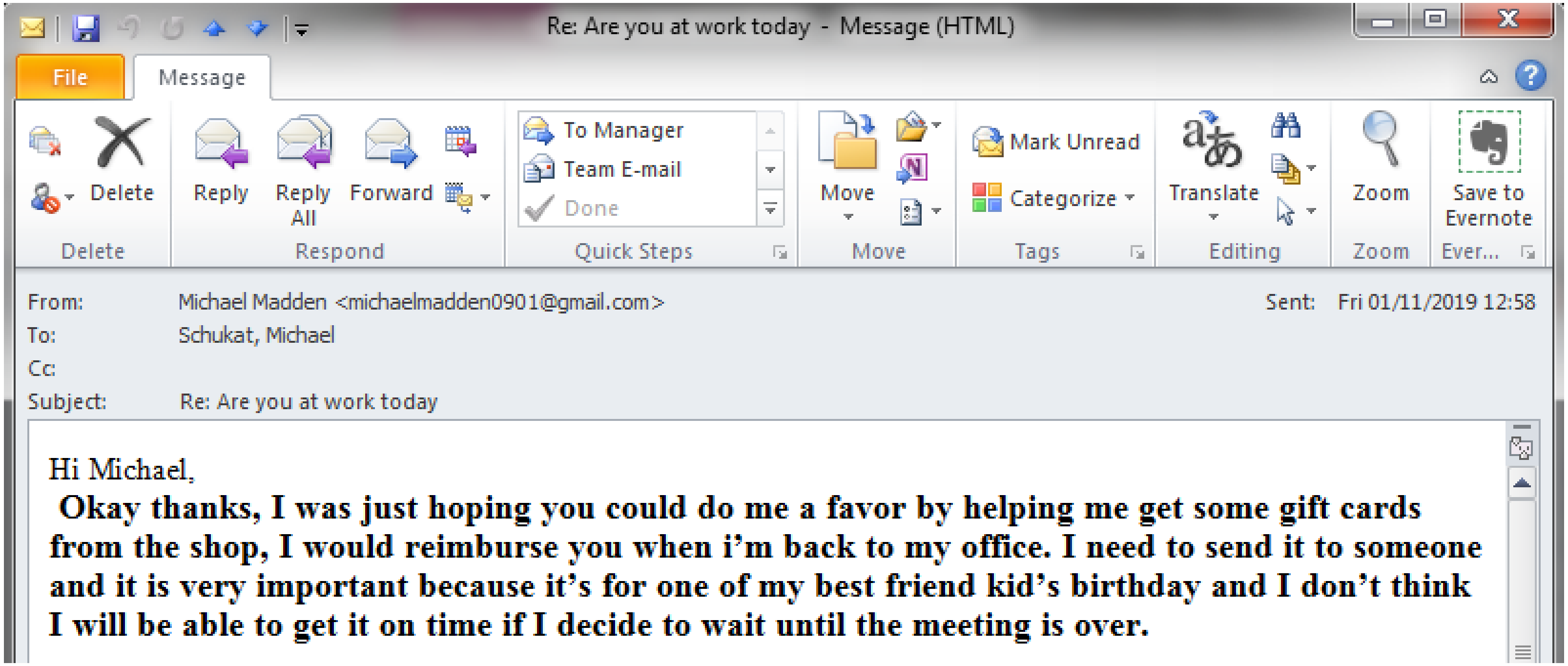
Example for Spear Phishing Email Trail #4



On Fri, Nov 1, 2019 at 1:56 PM Schukat, Michael <michael.schukat@nuigalway.ie> wrote:

> Ok, what I can I do?
>
> Regards,
>
> Michael

Example for Spear Phishing Email Trail #5



From: Michael Madden <michaelmadden0901@gmail.com>
Sent: Fri 01/11/2019 12:58
To: Schukat, Michael
Cc:
Subject: Re: Are you at work today

Hi Michael,

Okay thanks, I was just hoping you could do me a favor by helping me get some gift cards from the shop, I would reimburse you when i'm back to my office. I need to send it to someone and it is very important because it's for one of my best friend kid's birthday and I don't think I will be able to get it on time if I decide to wait until the meeting is over.

Example for Spear Phishing Email Trail

- Guess what happens next…

Smishing

- Smishing is short for SMS phishing and it works much the same as phishing
- Users are tricked into downloading a Trojan horse or virus <u>onto their phones </u>from an SMS text as opposed from an email onto their phone

Vishing

- Also called VoIP phishing
- It is the voice counterpart to phishing, e.g.
  - An email message asks the user to make a telephone call
  - Victims receive an unsolicited call
- Many different variations, see for example
  - https://www.youtube.com/watch?v=BEHl2lAuWCk
  - https://www.youtube.com/watch?v=PWVN3Rq4gzw

Alethe Denis, Winner of the Social-Engineering Competition @Defcon 2019

https://www.alethedenis.com/

FYI: Defcon

- DEF CON (also written as DEFCON, Defcon or DC) is one of the world's largest and most notable hacker conventions, held since 1993 annually in Las Vegas, Nevada

Pretexting

- Pretexting is defined as the practice of presenting oneself as someone else in order to obtain private information
- It is more than just creating a lie, in some cases it can be creating a whole new identity and then using that identity to manipulate the receipt of information
- Pretexting goes hand-in-hand with vishing

Quid Pro Quo

- Goes hand-in-hand with vishing
- Such an attack promises a service or a benefit based on the execution of a specific action
- Example:
  - A hacker attempts to contact via phone the employees of the target organisation then offers them some kind of upgrade or software installation
    They might request victims to facilitate the operation by disabling the AV software temporarily to install a malicious application

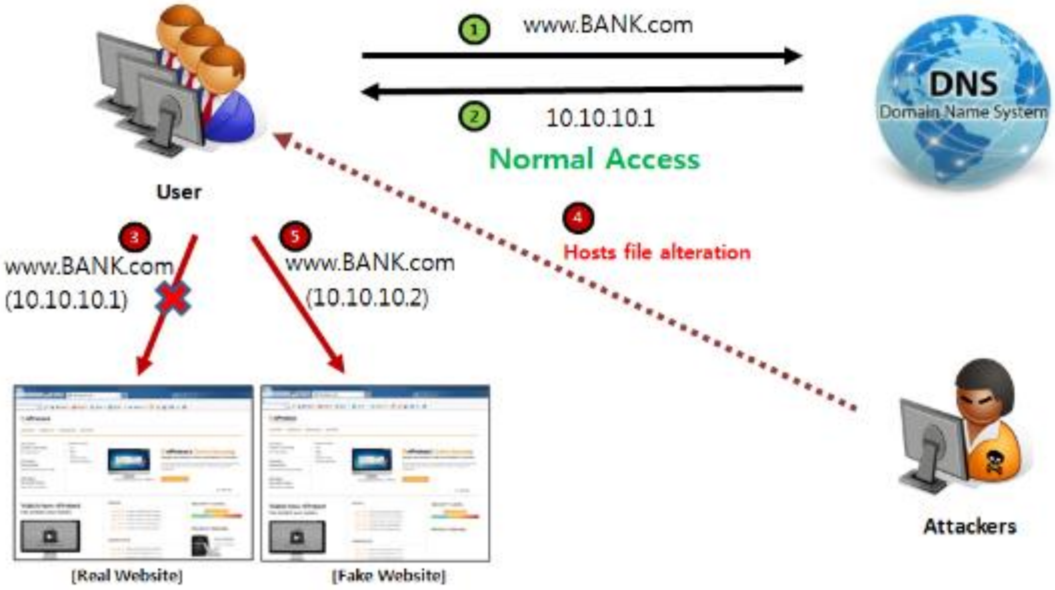
Watering Hole

- A watering hole attack consists of injecting malicious code into public Web pages of a site that the target uses to visit
  - https://www.youtube.com/watch?v=20jp-teI5no
- The attackers typically compromise websites within a specific sector that are typically visited by specific individuals of interest for the attacks
- Example: Blackboard ← → students

Pharming

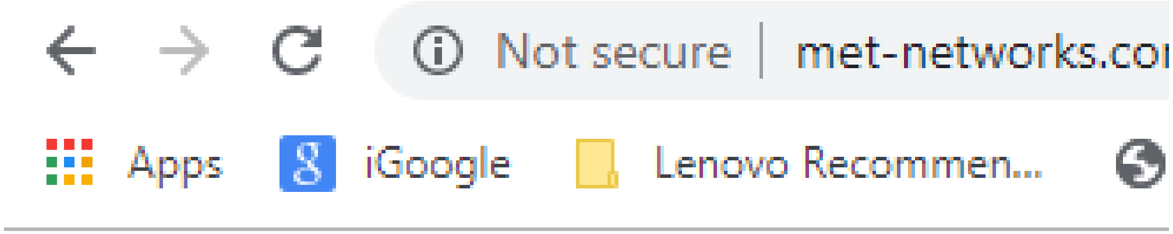
- Pharming scams redirect users to copies of popular websites where personal data like user names, passwords and financial information can be ‘farmed’ and collected for fraudulent use

Pharming via DNS Poisoning / DNS Spoofing



Domain Spoofing Pharming and how to detect it

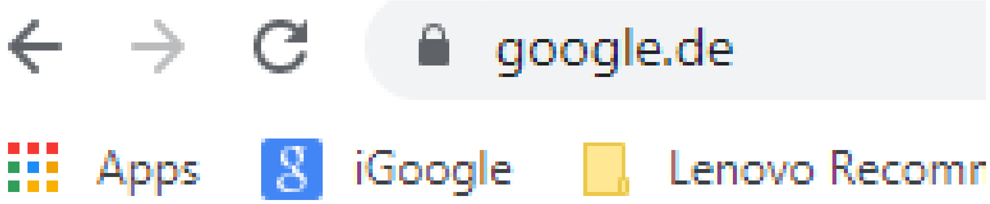
- Used domain spoofing (in which the domain appears authentic)



Not secure | met-networks.coı

Apps iGoogle Lenovo Recommen...

bad!

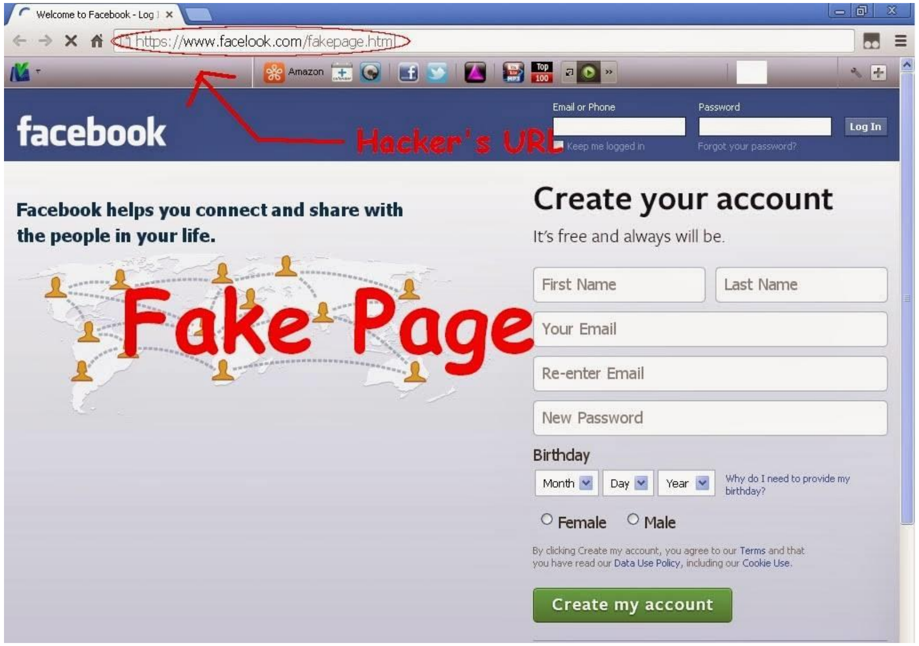


google.de

Apps iGoogle Lenovo Recomr

good!

Simple Pharming and how to detect it



Facebook helps you connect and share with the people in your life.

Create your account

It's free and always will be.

First Name

Last Name

Your Email

Re-enter Email

New Password

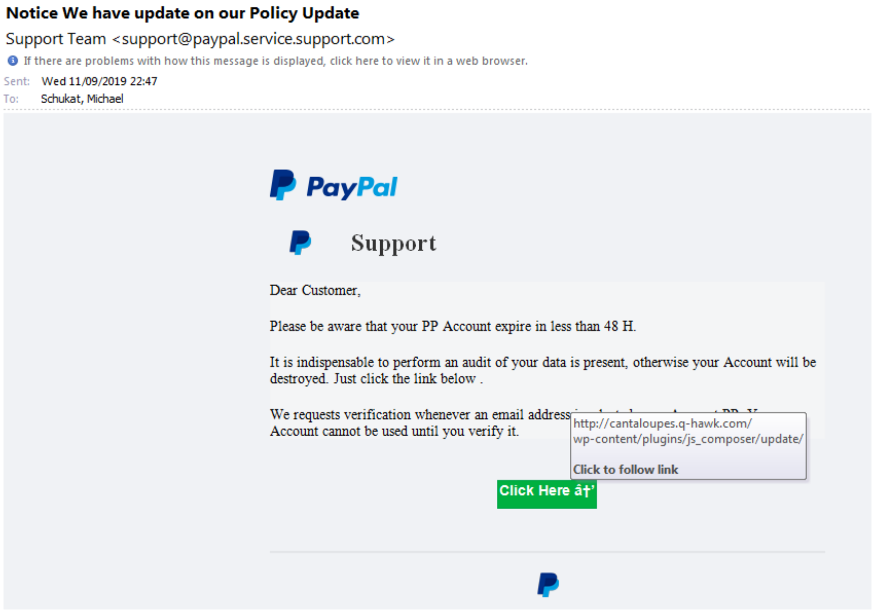
Birthday

Month Day Year Why do I need to provide my birthday?

○ Female ○ Male

By clicking Create my account, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Create my account



Notice We have update on our Policy Update

Support Team <support@paypal.service.support.com>

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

Sent: Wed 11/09/2019 22:47

To: Schukat, Michael

Dear Customer,

Please be aware that your PP Account expire in less than 48 H.

It is indispensable to perform an audit of your data is present, otherwise your Account will be destroyed. Just click the link below .

We requests verification whenever an email address
Account cannot be used until you verify it.

http://cantaloupes.q-hawk.com/wp-content/plugins/js_composer/update/

Click to follow link

Baiting

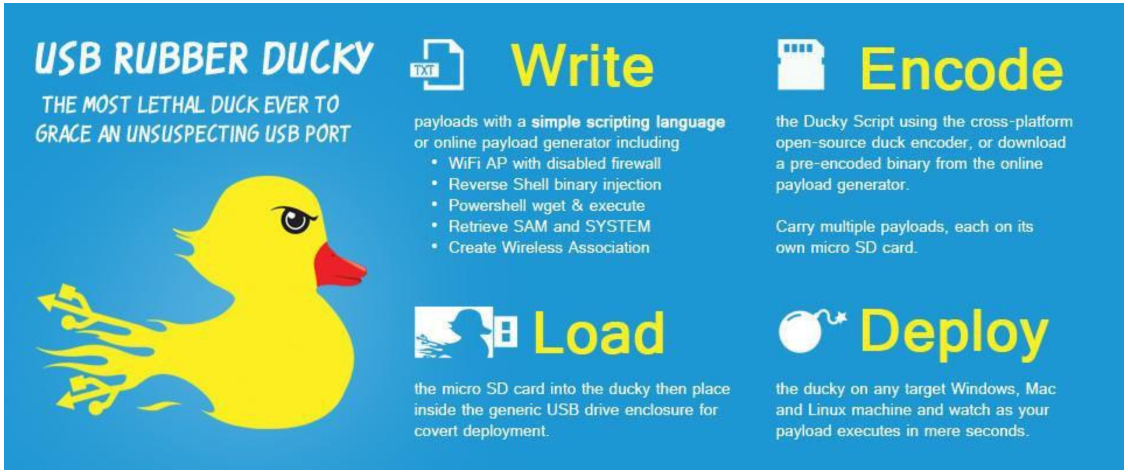
- Baiting that exploits the human’s curiosity
- Example USB drop attacks
  - Leave infected USBs tokens in the parking lot of a target organization and wait for internal personnel insert them in the corporate PC
  - See https://www.redteamsecure.com/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives/
- Funny: https://www.youtube.com/watch?v=GQMsOH-yDBU

USB Baiting

- USB baiting exploits the human's curiosity
  - You find a memory stick and want to know what's stored in it
- Example (USB drop attack): Leave infected USBs tokens in the parking lot of a target organization and wait for personnel inserting them in a corporate PC; three things may happen:
  - The user clicks on one of the files on the drive, which unleashes a malicious code that automatically activates upon viewing and can download further malware from the Internet
  - Alternatively the user is directed to a phishing website
  - HID (Human Interface Device) spoofing – see next slide

USB Baiting and HID spoofing

- The USB stick will trick the computer into thinking a keyboard is attached. When plugged into a computer, it injects keystrokes to command the computer to give a hacker remote access to the victim's computer
- USB Rubber Ducky – the most lethal duck ever!
- https://www.youtube.com/watch?v=sbKN8FhGnqg



USB RUBBER DUCKY

THE MOST LETHAL DUCK EVER TO GRACE AN UNSUSPECTING USB PORT

Write

payloads with a **simple scripting language** or online payload generator including
- WiFi AP with disabled firewall
- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

Encode

the Ducky Script using the cross-platform open-source duck encoder, or download a pre-encoded binary from the online payload generator.

Carry multiple payloads, each on its own micro SD card.

Load

the micro SD card into the ducky then place inside the generic USB drive enclosure for covert deployment.

Deploy

the ducky on any target Windows, Mac and Linux machine and watch as your payload executes in mere seconds.

Tailgating aka Piggybacking

- Attacker seeking physical entry to a restricted area which lacks the proper authentication
- Example:
  - An attacker can walk in behind a person who is authorised to access the area
  - In a typical attack scenario, a person impersonates a delivery driver or a caretaker who is packed with parcels and waits when an employee opens their door