OCIO - ES

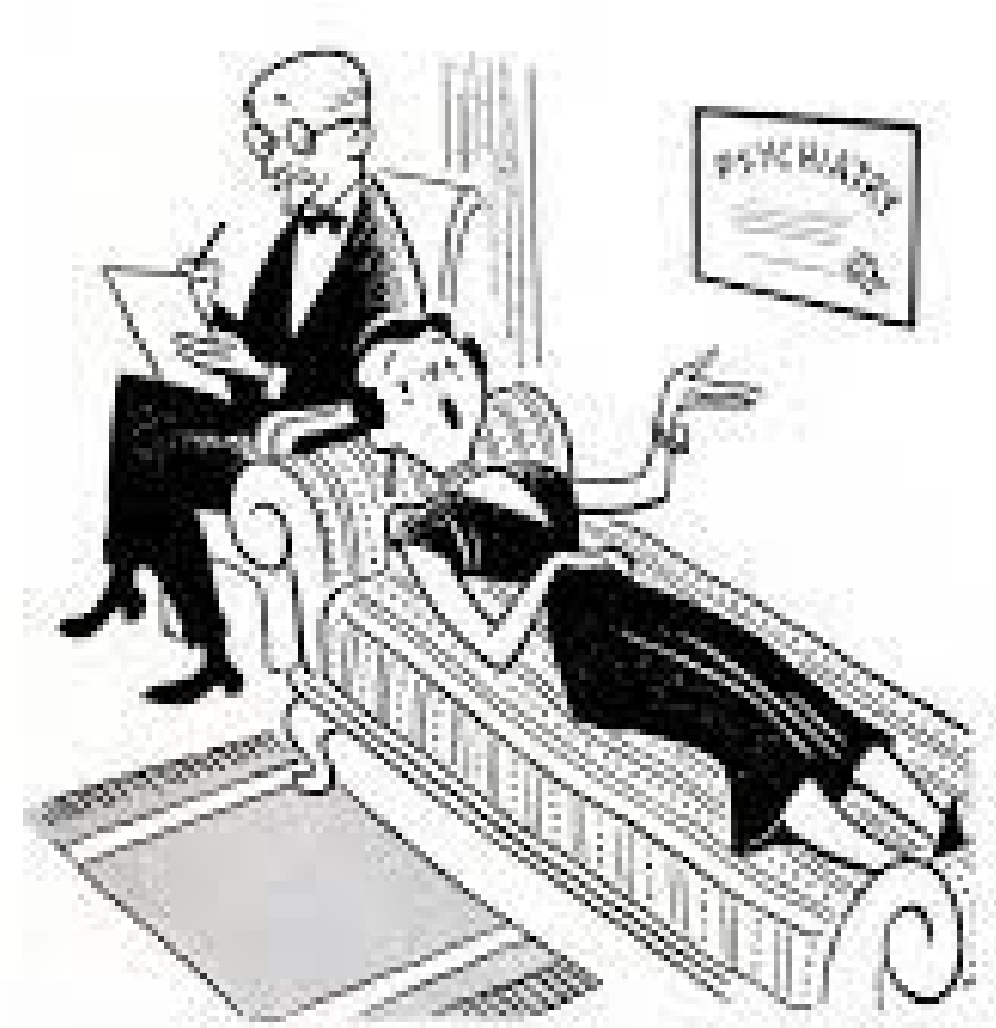
Please put down your phishing pole... **2021**

BRITISH COLUMBIA | Ministry of Citizens' Services

Agenda

- What does Phishing look like to the victim?
- What is “phishing”
- What is “Social Engineering”
- Why does it work?
- What to look for?
- Why is it so hard to prevent?

Testimonial…



As recited by Jarin James…

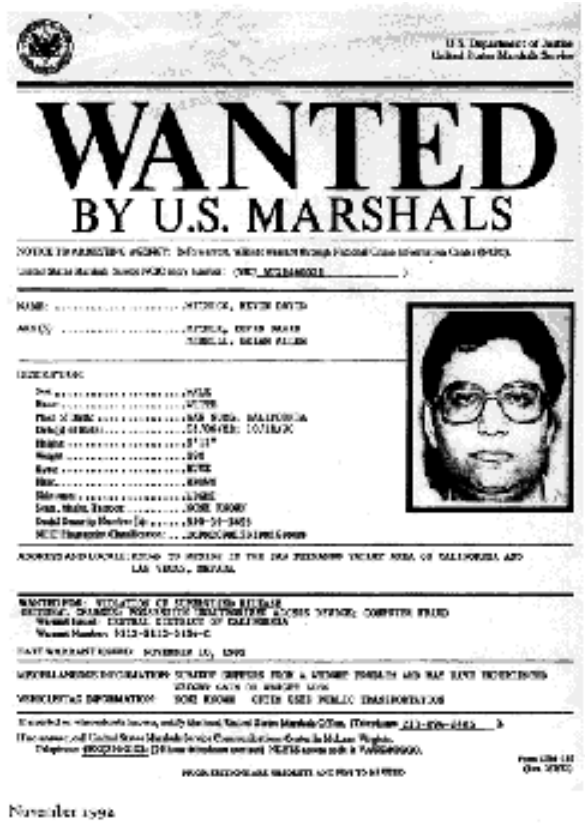
Phishing – a definition

- phish·ing | \ ˈfi-shiŋ \

: the practice of tricking Internet users (as through the use of deceptive email messages or websites, or text) into revealing personal or confidential information which can then be used illicitly

(or trick the user into installing software, known as Malware, that will give the attacker access to their system or data).

Social Engineering



Phishing is a form of Social Engineering

As old as the human race itself.

Relies on the way the human brain processes information and associated emotional response

Can misuse automatic processing of clues including:

- Urgency
- Familiarity
- Trust

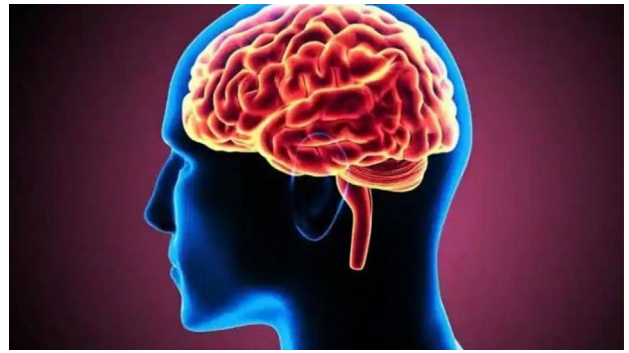
https://ideas.ted.com/why-we-fall-for-phishing-emails-and-how-we-can-protect-ourselves/

Why does "*phishing*" work so well?

Perception of Trust

Often the message appears to come from a source that is trustworthy.

Ex: Your boss, your bank, your employer, a friend/colleague (who has been compromised or faked)…



Urgency

Appears to require quick action or is a ***threat***

Ex: Help needed, or threat to your finances,…

Curiosity

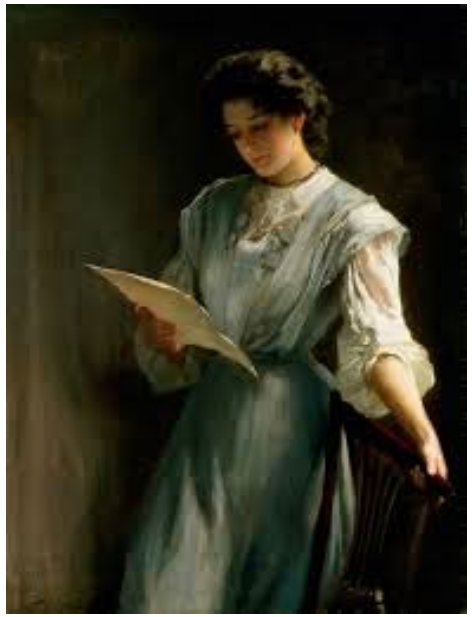
The topic hinted at seems very interesting to the recipient

Ex: financial windfall, mysterious charge, a new account in your name has been opened, …

What to look for

- First, lets talk about the parts of a email message…
- All information is provided by the “Sender” except the “Date”.

Sender (Display vs. Actual)
Date (When was it received in the mail system)
Recipient (who got it?)
Subject (What do they want to tell you in summary?)
Body
URL Links (Display vs. Actual)
Attachments (filename.extension)



[Anomali ThreatStream] Your daily Threat Model digest

Anomali ThreatStream <info@anomali.com>
To Land, Dale CITZ:EX

Reply | Reply All | Forward | ...

Sat 2021-10-16 12:37 AM

^ Outlook

Gmail >

Cybersecurity Careers Awareness Week: Learn How to Level Up Your DFIR Career

Inbox ×

Magnet Forensics <sales@magnetforensics.com> Unsubscribe

11:25 AM (3 hours ago)

to me

from:	**Magnet Forensics** <sales@magnetforensics.com>
to:	dale.land@gmail.com
date:	Oct 18, 2021, 11:25 AM
subject:	Cybersecurity Careers Awareness Week: Learn How to Level Up Your DFIR Career
mailing list:	<7214043.xt.local> Filter messages from this mailing list
mailed-by:	bounce.s7.exacttarget.com
signed-by:	magnetforensics.com
security:	Standard encryption (TLS) Learn more

Clue #1: SENDER

As noted before, the SENDER has **2 parts**; The display name (provided by the sender… "Mary Trustworthy") AND (the actual sender, i.e. something@somewhere.domain)

Examples:

Dale Land (dale.land@almostgov.bc.ca)

Mobile devices just show "Dale Land" normally.

Most people are used to just looking at the display name.

LOOK CLOSELY at the real sender address.

Danger: in Phishing, one or both can be BOGUS…

Clue #2: DATE

- The date the message was received is timestamped by recipients (i.e. your) mail system gets it. It is accurate.

Examples:

Email from your boss, received November 2 @ 2AM?

Danger: If you get mail from a trusted person (friend, co-worker, boss). Is the middle of the night reasonable?

Does your trusted company (say Bank) normally send you these kinds of messages?

Clue #3 RECIPIENT

forme

- Who is the email addressed to?

Choices are:

1. <blank>. That means they don't really know who you are.
   Ignore… (mostly, sometimes legit email comes to you as a BCC)
2. They got your display name wrong, but email address right.
   Probably from a SPAM email list they acquired.
   Ignore…
3. Your actual name. Your real email address.
   Could be legit, but Check the first 2 clues closely.

Clue #4 SUBJECT

- Does the subject cause an immediate emotional response?

Example:

“RBC has credited your account $643.37”

“New cool game – play for free”

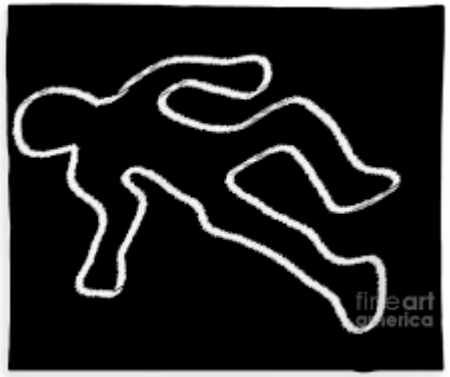
“Help!”

“CRA Notice of Assessment: $2,323.00 due”

“Action Required”

“COVID Exposure Notice”

Clue #5: BODY



- The body of the message may try and convince you that a reply is required or to click on the included link or open the attached file.

BRITISH COLUMBIA | Ministry of Finance

2021 PROPERTY TAX NOTICE

issued under the Taxation (Rural Area) Act

Registered Taxpayer,
Our records show you are overdue on paying your tax assessment of $10,325.23.
Please click on the following link to access your assessment and make payment.
BC Assessments Notice *(which if you hover goes to bcassessments.nl)*

URL Links

- Embedded links (in the body of messages have **2 parts**: Display part, actual Link. You can see the actual link by hovering over the Display link (without clicking).

Example:

Urgent: Phishing Action Required

Land, Dale CITZ:EX
To Land, Dale CITZ:EX

3:36 PM

You are being phished. You absolutely should click on the link below to go to a fake login screen so you can give me your Bank's log in information.

RBC Login Screen

Thanks

RBC Accounts Department

Attachments

- Attachments can be *anything*
- PDF, MS Office Doc, Web Page, Executable.
- Be Careful: Windows may not show the final (and valid) extension (if there are multiple).

Example: Bank Statement.pdf.exe will only show

Bank Statement.pdf, but will execute as a program if you click on it…

Conclusion: Why so hard to prevent…

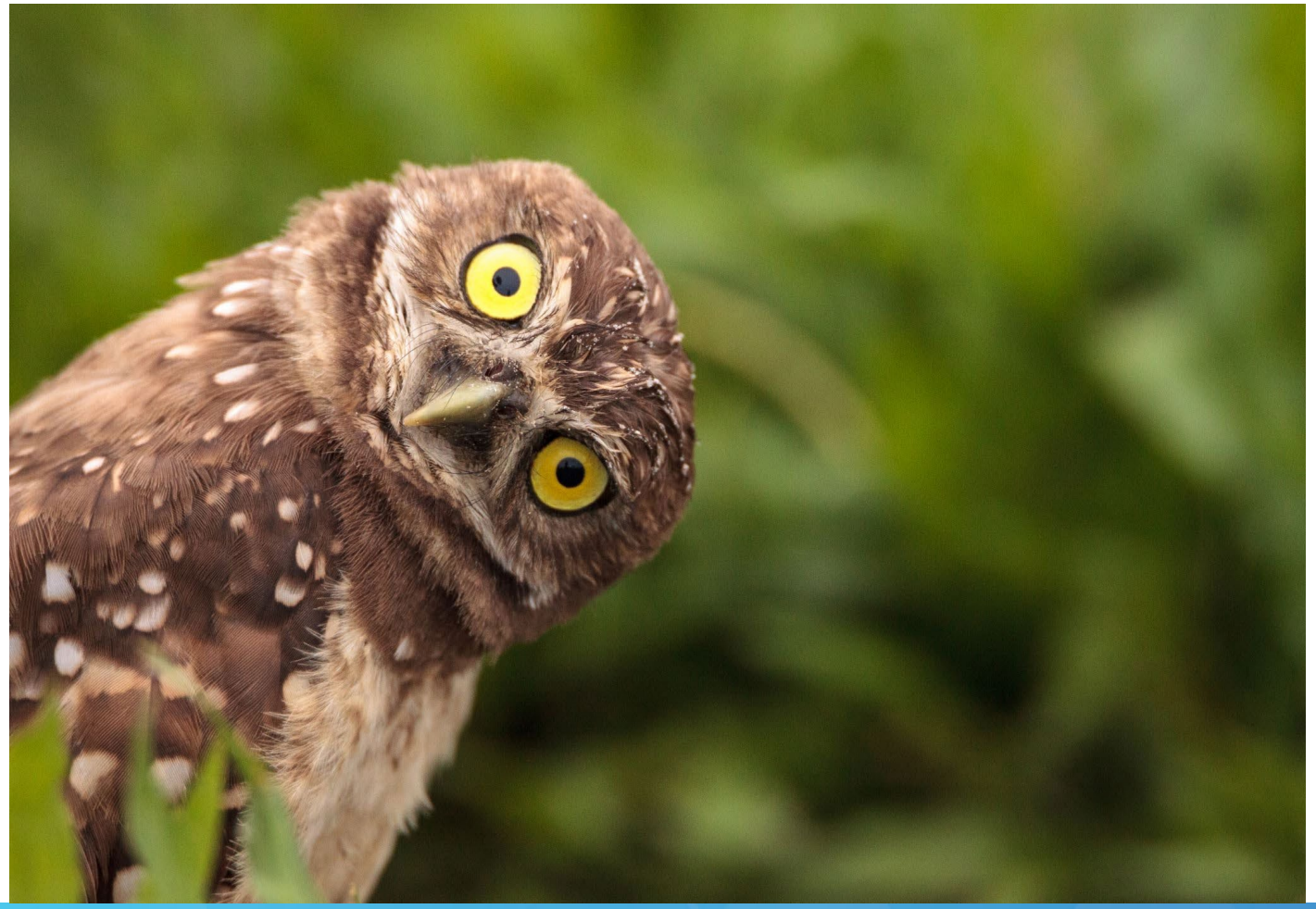
Because most of the Clues are only understandable by HUMANS.

Better email systems can look at *patterns*:

- Reputation information on sending email servers,
- Patterns on external email to multiple recipients,
- Reputation information when you click on a link
- Attachment type blocking

Fraudsters are creative too, they are trying to evade protections…

Be Safe, Be paranoid when reading email.



From Urgent: Fraudlent activities [redacted]

Subject **Office365**

To [redacted]

[redacted]

Reply | Reply All | Forward | More

10/18/2021, 12:21 PM

Office 365

We are unable to verify your account Microsoft office information on file for your registration

As a result, your account will not renew and will suspended

if you'd like to renew your account please fill out the Account Verification Form at least

48 hours from now, if you don't verify your account, your account will be suspended.

VERIFICATION

Microsoft Corporation

One Microsoft Way, Redmond, WA 98052, USA

This email is intended for ##EMAIL##

Microsoft respects your privacy. Please read our Privacy Statement.

For people in Canada

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager.

Microsoft Canada Inc.

1950 Meadowvale Blvd.

Mississauga, ON L5N 8L9 Canada