

CYBER SECURITY AWARENESS

PROTECTING
YOURSELF IN A
CYBER WORLD

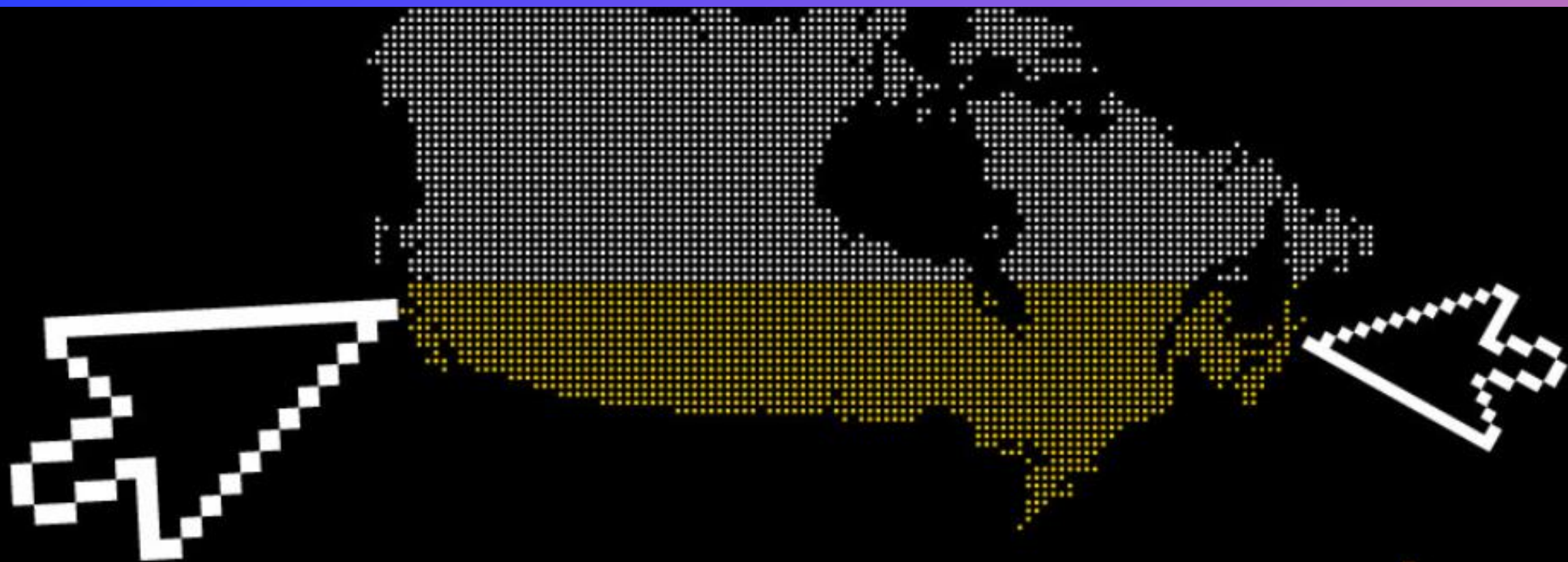


Gavin Taylor, CISSP



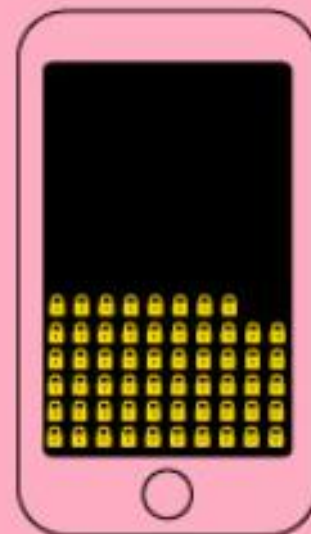
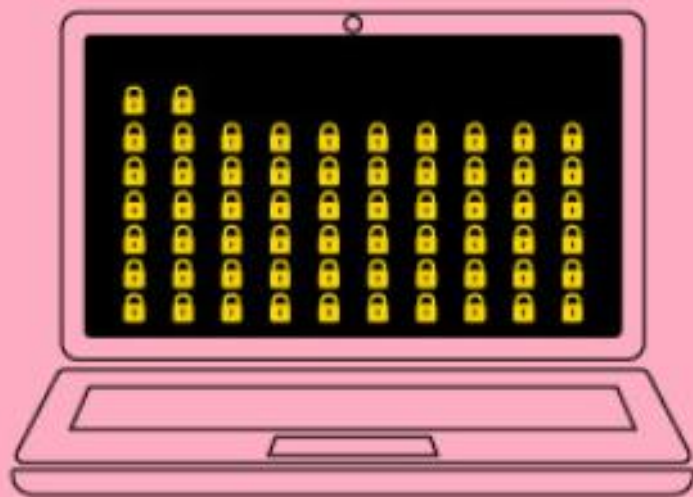
AGENDA

Social Engineering – How cyber scams work
Different types of phishing
Phishing examples
Processes and practices



41% OF CANADIANSⁱ

BELIEVE IT IS UNLIKELY THAT THEIR
PERSONAL INFORMATION COULD BE
COMPROMISED ONLINE



62%ⁱ

**SAY THEY "TAKE
STEPS TO PROTECT
THEMSELVES
ONLINE"**

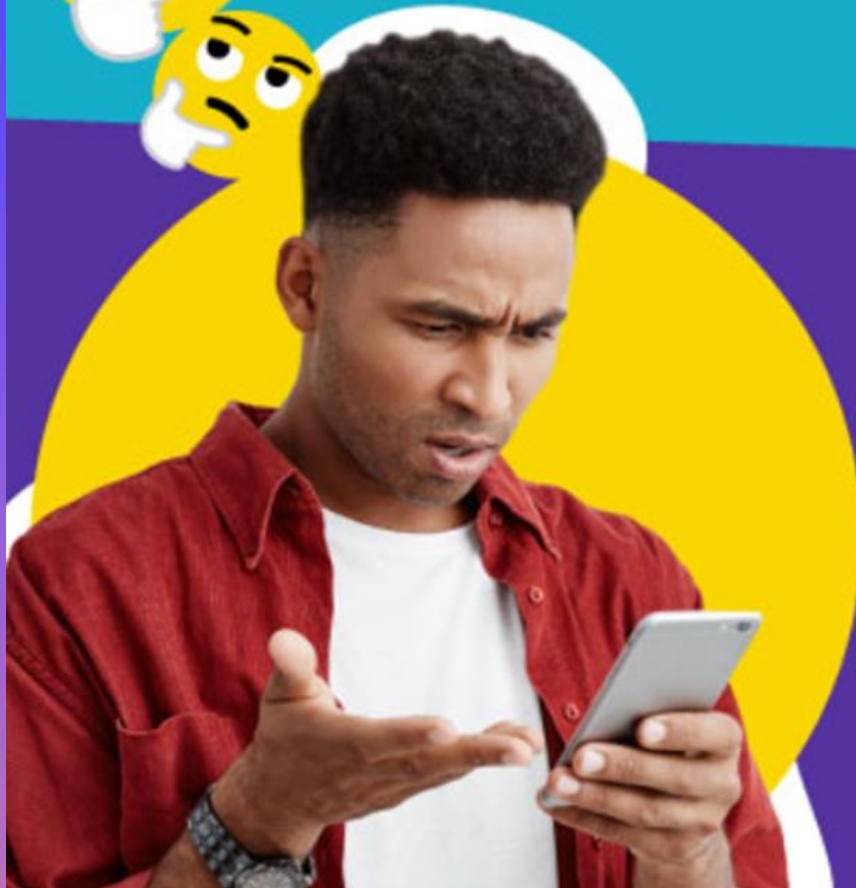
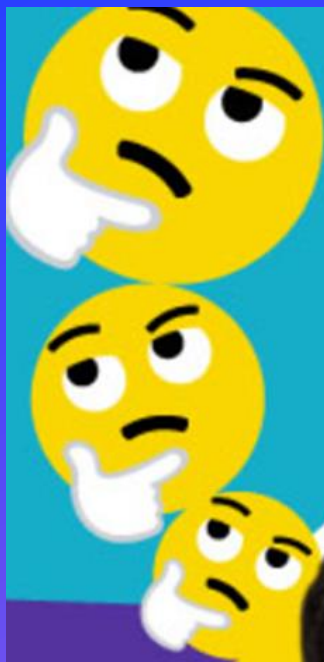
58%ⁱ

**SAY THEY "DON'T
DO ANYTHING
RISKY ONLINE"**

**BUT MANY CYBER THREAT
ACTORS TRY TO TRICK
PEOPLE INTO **GIVING UP**
INFORMATION INSTEAD
OF TRYING TO ATTACK
THEIR DEVICES.**



WHY DO CYBER SCAMS TRICK US?



It can seem impossible to believe that cyber criminals can get information just by asking for it – but if it were impossible, we wouldn't be here. Cyber threat actors have many scams to get people to give them what they want. Knowing about how they work can help you protect your information online.

THIS IS CALLED
SOCIAL ENGINEERING



SO, HOW DOES **SOCIAL** **ENGINEERING** WORK?



1

**A CYBER CRIMINAL
DOES RESEARCH ON**

SEARCH ENGINES

SOCIAL MEDIA

**to learn more about
you or your company.**

2

**THEY SEND YOU A
MESSAGE THAT LOOKS
LIKE IT'S FROM**

A FRIEND

YOUR BOSS

A FAMILIAR COMPANY

or another trusted source.

3

THEY TRICK YOU INTO SENDING SENSITIVE INFORMATION, LIKE

PASSWORDS

FINANCIAL DATA

CREDIT CARD NUMBERS



- **Hackers leverage social engineering in as much as 90% of all cyberattacks**
- **Social engineering is effective because it relies on the human tendency to trust, fear, or oblige to orders**
- **Two of the biggest cyberattacks of 2023 were caused by social engineering**

SOCIAL ENGINEERING IS

TARGETED AND SOPHISTICATED

AND **ANYONE** CAN FALL FOR IT.



(YEAH,
EVEN **YOU.**)



Phishing

@

Phishing refers to any attempt to steal information, whatever the means

+

•

○

Phishing is a common tactic that cyber criminals use to steal personal and financial information from you

+

○

•

Phishing messages can come in almost any form: Emails, text messages, social media direct messages, or phone calls

- + In most cases, cyber criminals' phishing campaigns are untargeted attempts to solicit**
- personal details by casting as wide a net as possible to get people to respond**



How many of you have had calls saying they're from Microsoft Support, the CRA or calling about your credit card

WHAT ARE THE DIFFERENT FORMS OF PHISHING?





SMISHING

Is a phishing attempt through SMS (text message)



SPEARFISHING

- Is a hyper-targeted phishing attempt in which a message is designed to sound like it's coming from a source you know personally



WHALING

Is a phishing attempt aimed at a high-profile target such as a senior executive or other high-ranking official in an organization or government department



SPOOFING

Involves creating a fake website to get someone to share their personal information

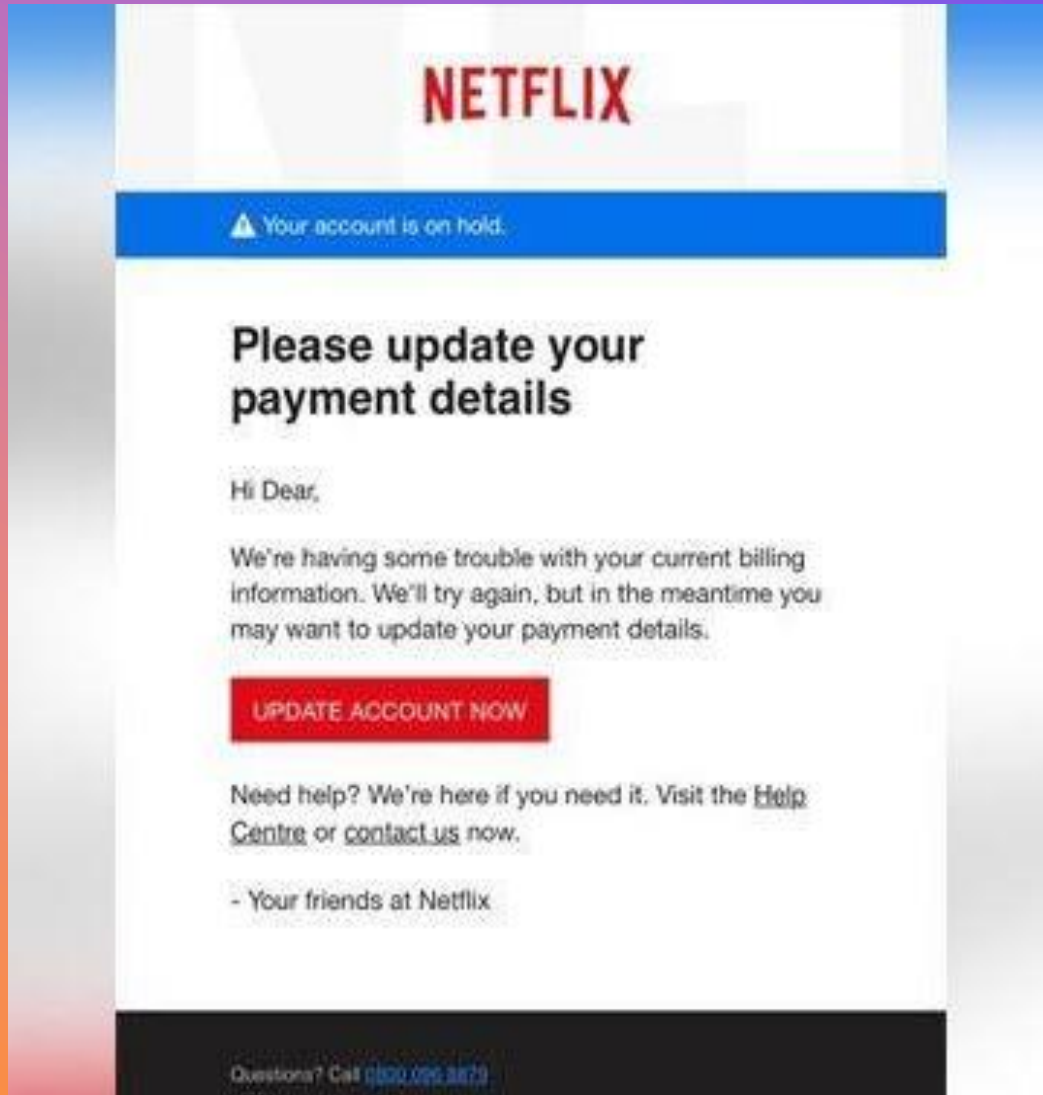
Dangers of falling for a phishing campaign

Phishing scams can be very costly

Cyber criminals can use the information that they gather to access your email, steal your financial information, open accounts in your name, steal your money or steal your identity

They could sell your information to other scammers

Scammers launch thousands of phishing attacks like these every day — and they're often successful



Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company's logo in the header:

- The email has a generic greeting
- The email says your account is on hold because of a billing problem
- The email invites you to click on a link to update your payment details

EXAMPLES OF PHISHING EMAILS



REQUEST



Marian Heil <teambookkeepers@gmail.com>

To [REDACTED]@gardenontario.org



Mon 2022-09-26 11:15 AM

Hello,

I am trying to set up an E-Transfer or (BITCOIN TRANSFER) in the amount of \$2,850 for an expense, also I will need to visit the bank to set it up. I would like to know if you can initiate the transfer from your personal account and put it in a request for reimbursement. Let me know so I can send you necessary details thanks.

Regards,

Marian Heil



REQUEST



Marian Heil <teambookkeepers@gmail.com>

To [REDACTED]@gardenontario.org



Mon 2022-09-26 11:15 AM

Hello,

I am trying to set up an E-Transfer or (BITCOIN TRANSFER) in the amount of \$2,850 for an expense, also I will need to visit the bank to set it up. I would like to know if you can initiate the transfer from your personal account and put it in a request for reimbursement. Let me know so I can send you necessary details thanks.

Regards,
Marian Heil



From: Marian Heil <treasurerboard55@gmail.com>

Subject: REQUEST

Date: September 19, 2022 at 11:48:22 AM EDT

To: [REDACTED]@gardenontario.org

Hi,

I am trying to set up an E-Transfer in the amount of \$1,880 for an expense, also i will have to visit the bank to set it up as we don't E-transfers or pay bills online as we have a 2 signature account, I would like to know if you can initiate the E-transfer from your personal account? I will send you a reimbursement cheque in your name tomorrow evening let me know so i can send you the details.

Regards,

Marian Heil

From: Marian Heil <treasurerboard55@gmail.com>

Subject: REQUEST

Date: September 19, 2022 at 11:48:22 AM EDT

To: [REDACTED]@gardenontario.org

Hi,

I am trying to set up an E-Transfer in the amount of \$1,880 for an expense, also i will have to visit the bank to set it up as we don't E-transfers or pay bills online as we have a 2 signature account, I would like to know if you can initiate the E-transfer from your personal account? I will send you a reimbursement cheque in your name tomorrow evening let me know so i can send you the details.

Regards,

Marian Heil

From: **Sharlene Desjardins** <boards@disroot.org>
Date: Mon, Oct 9, 2023, 9:53 a.m.
Subject: QUICK ATTN :
To: <secretary@gardenontario.org>

Good Day Kelly,

I hope you are doing well .

Are available to carry out official duties for me today.

Regards,
Sharlene Desjardins.

- **Wrong sender email address**
- **Grammatical errors**
- **Out of character for the OHA President**

From: **Shirlene Badenach** <shirlene.badenach@bigpond.com>

Date: Sun, Sept 17, 2023, 9:21 p.m.

Subject: OHA Awards Nomination Form 2023

To: <ohasecretary@gmail.com>

<https://form.jotform.com/232288785405869>

Sent from my iPhone

- **Wrong sender email address**
- **Link to a web-based document which could contain malware**

Notifications ⌵ Inbox x



Walmart info_1igti4Q5soTO@kxwuqdcauqni.free.do [via wildcardplug.store](#)
to gtaylor448LY, gtaylor448iZ

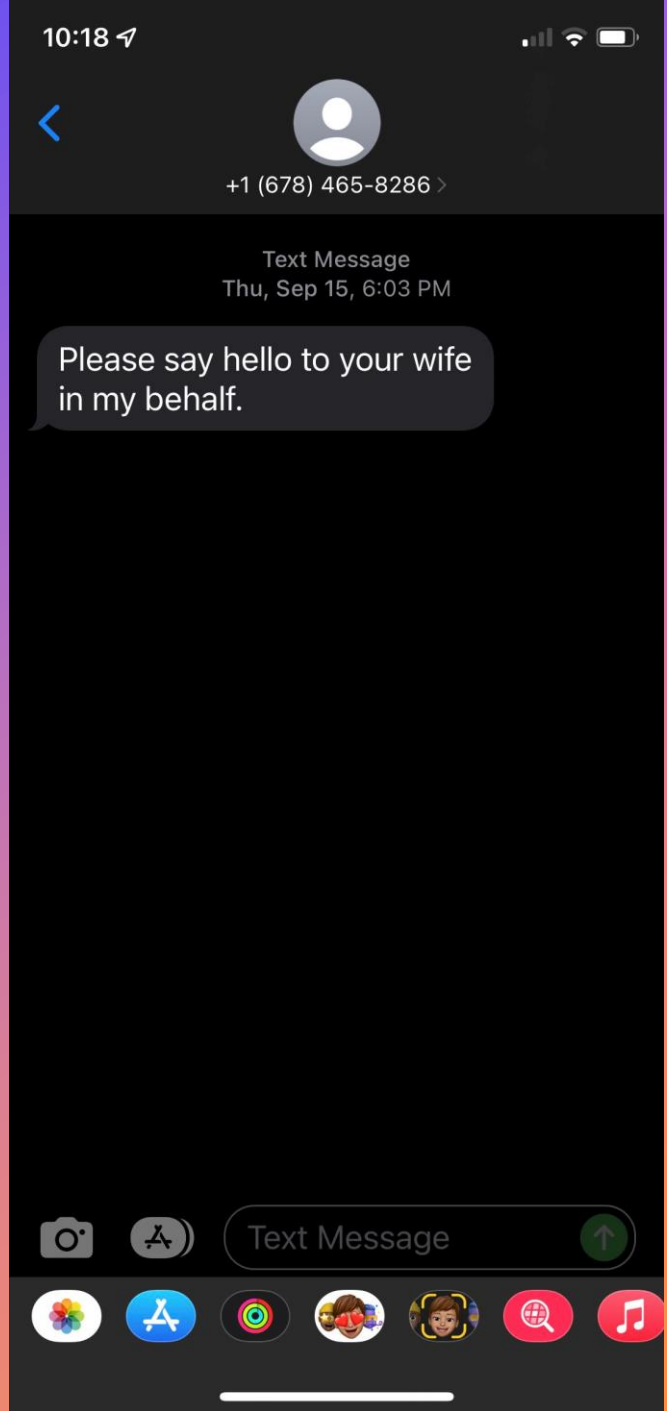
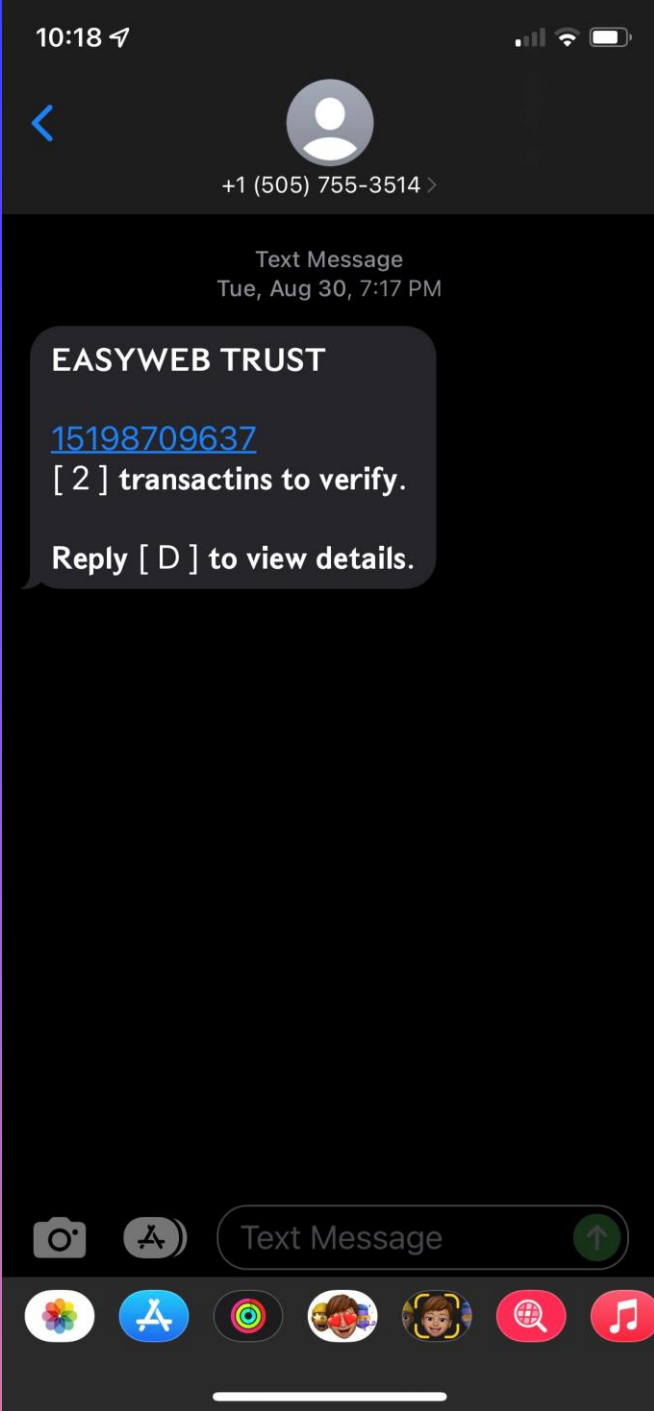
Sep 28, 2022, 12:15 PM (1 day ago)

from: **Walmart**
<info_1igti4Q5soTO@kxwuqdcauqni.free.do>
[via wildcardplug.store](#)
to: gtaylor448LY@aol.com
cc: gtaylor448iZ@aol.com
date: Sep 28, 2022, 12:15 PM
subject: Notifications
mailing list: <.7289367.xt.local> [Filter messages from this mailing list](#)
mailed-by: wildcardplug.store
security: Standard encryption (TLS) [Learn more](#)

- **Wrong sender email address**
- **Multiple email address variations**

SMISHING EXAMPLES

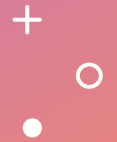




How to protect yourself from phishing campaigns

- + There is no simple way to ensure you are 100 per cent protected against phishing campaigns
- - Phishing campaigns are becoming increasingly elaborate, and the growth of digital platforms, like social media, have given cyber criminals many opportunities to reach victims


7 RED FLAGS YOU SHOULD CHECK FOR



Notifications ▾ [Inbox](#)




Walmart info_1tgi4Q5so1D@kxwuqdcuqni.free.do [walmartcardplug.store](#)
to gtylor448LY, gtylor448IZ ↘



ANSWER & WIN
A Brand New
Ultimate Nonstick Cookware

GET STARTED



You have been chosen to participate in our Loyalty Program for **FREE!**
It will take you only a minute to receive this fantastic prize.

If you no longer wish to receive these emails, you may unsubscribe by clicking here or by writing to 6130 W. Flamingo Rd., Las Vegas NV 89119

Architecture Improve - 165 Bradley Ray Dr Moadview, AZ 86444 US
If you don't want to receive this type of message, you can [unsubscribe](#) from this list.

1. URGENT OR THREATENING LANGUAGE

- +
 - Real emergencies don't happen over email.

○

Look out for:

- Pressure to respond quickly
- Threats of closing your account or taking legal action

+

○

•

2. REQUESTS FOR SENSITIVE INFORMATION

Anyone asking for personal information over email or text probably shouldn't be trusted with it, anyway.

Look out for:

- Links directing you to login pages
- Request to update your account information
- Demands for your financial information, even from 'your bank'.

3. ANYTHING TOO GOOD TO BE TRUE

+ Winning a lottery is unlikely. Winning a lottery you didn't enter is **impossible!** +

•
○
Look out for:

- Winnings from contests you've never entered
- Prizes you have to pay to receive
- Inheritance from long-lost relatives

4. UNEXPECTED EMAILS

• + Expect the unexpected, and then send it right to the **trash**. + ○

○ **Look out for:**

- Receipts for items you didn't purchase
- Updates on deliveries for things you didn't order

5. INFORMATION MISMATCHES

Searching for clues in phishing email puts your love of true crime podcasts to good use.

- +
 - - **Look out for:**
 - Incorrect (but maybe similar) sender email addresses
 - Links that go to official websites
 - Spelling or grammar errors, beyond the odd typo, that a legitimate organization wouldn't miss



6. SUSPICIOUS ATTACHMENTS

Attachments might seem like gifts for your inbox. But just like real gifts, they're not always good...

Look out for:

- Attachments you didn't ask for
- Weird file names
- Uncommon file types

7. UNPROFESSIONAL DESIGN

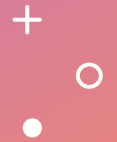
For some reason, hiring a graphic designer isn't on a cyber criminal's priority list.

- - **Look out for:**

- Incorrect or blurry logos
- Company emails with little, poor or no formatting
- Image-only emails (no highlightable text)

IF YOU SPOT ANY OF THESE RED FLAGS IN A MESSAGE:

- +
- - • Don't click any links
 - Don't reply or forward
 - Don't open attachments



If you're uncertain?

- Question it
- Reach out to your peers and validate

+

If you don't know?

- Ask
- Call and check with one of your board members

+

○

•

Have processes and follow them

PROCESSES CAN SAVE YOU

Have processes in place which outline how you handle finances

- + • **Set spending limits for the board that don't require approval**
- **Set board spending limits which require society approval**
- **Ensure you require multiple signatures or approvals before spending or paying out reimbursements**
- **Have a process for emergency or unbudgeted expenditures. Ensure they require disclosure to the members and a majority vote**



+

o



THANK YOU



Some slides courtesy of the Canadian Centre for Cyber security

QUESTIONS

If you have questions, please email them to Kelly Taylor, OHA Secretary at:

OHASECRETARY@GMAIL.COM