



Scammers and Other Invasive Species

Recognize Them

Deal With Them

Al Williams

April 6, 2023

Part 1

Scammers –

Scamming at Home

Part 2

Scammers –

Scamming Our Online Accounts

Part 3 – Invasive Species

The situation is similar to an arms race
scammers and invasive species look for
ways to get our information and we
look for ways to block them.

The scammer's reasons

Money

Political motivation

The scammer's point of view

Scamming is the easiest way to get a person's data, almost no knowledge of technology is needed

It's difficult for scammees to prevent because scamming uses human psychology to gain access

Source: <https://www.ibm.com/topics/social-engineering>

How scammers use social engineering

Pose as a trusted brand

Pose as a government agency or authority figure

Induce fear or a sense of urgency

Appeal to greed

Appeal to helpfulness or curiosity

Source: <https://www.ibm.com/topics/social-engineering>

What scammers do once they have access

Install remote desktop access application

May install a keylogger

May install malware

Scammers want

Login credentials – username and password

Credit card numbers

Bank account numbers

Social Security numbers

Source: <https://www.ibm.com/topics/social-engineering>

Scammers use stolen information to

Make purchases

Apply for loans

Apply for unemployment benefits

As the first stage of a larger-scale cyberattack

And more

Source: <https://www.ibm.com/topics/social-engineering>

Scammers try to create breaches into our data using

Phones

Email

Text messages

Websites

Source: <https://www.ibm.com/topics/social-engineering>

Landline Phones

Scam Phone Calls – Responding

Use Caller ID to screen callers

Use a Smart Call Blocker phone if you want to further deal with annoying calls

Never say “Yes” during a phone call with a stranger

Scam phone calls are also known as Vhishing

Scam Phone Calls – Smart Call Block Options

1. Block phone number by pressing “Block”
2. If Family, Friend, or Invited Guest, Press #, Otherwise, Hang Up
3. Ask Caller to announce name, then press #
4. Use either an Allow List or a Block List

Suggested: AT&T BL102 Cordless Phone, may have multiple handsets

Cell Phones

Cell Phones

Carriers are actively blocking scammers

Malwarebytes for iOS – May be used anywhere

Malwarebytes Call Protection for Android – UK and Ireland only

Email

Where do these species get our
email addresses?

The Global State of Digital – October 2022

Total World Population:	7.99 Billion	
Unique Mobile Phone Users:	5.48 Billion	68.6%
Internet Users:	5.07 Billion	63.5%
Active Social Media Users:	4.74 Billion	59.3%

Source: <https://wearesocial.com/us/blog/2022/10/the-global-state-of-digital-in-october-2022/>

HaveIBeenPwned.com

Unique Mobile Phone Users:	5.48 Billion
Pwned accounts:	12.48 Billion
Unique passwords:	306 Million

“While HIBP is kept up to date with as much data as possible, it contains but a small subset of pwned accounts...”

Source for Cell Phone Users: <https://wearesocial.com/us/blog/2022/10/the-global-state-of-digital-in-october-2022/>
Source for accounts and passwords: <https://haveibeenpwned.com>

Email – Phishing

Email Phishing

We should assume that our email addresses have been exposed in a data breach

Use <https://HaveIBeenPwned.com> to verify that your email address was exposed and what other information was exposed, especially passwords

Email Phishing

If the password for an account was exposed in a data breach, change it using a password generator or roll dice – don't make up your own password, humans are not good at making unique passwords

Passwords should have at least 19 characters – upper and lower case letters, numbers and symbols

Email Phishing

Use an email masking service for accounts

An email masking service allows the creation of a unique email address for that account. The service forwards the email to your actual email address.

Example:

stungbullish587@simplelogin.com

Email Phishing

Possible email masking services:

Anon

DuckDuckGo

FastMail

Firefox Relay

SimpleLogin

Suggested: SimpleLogin – free and paid options

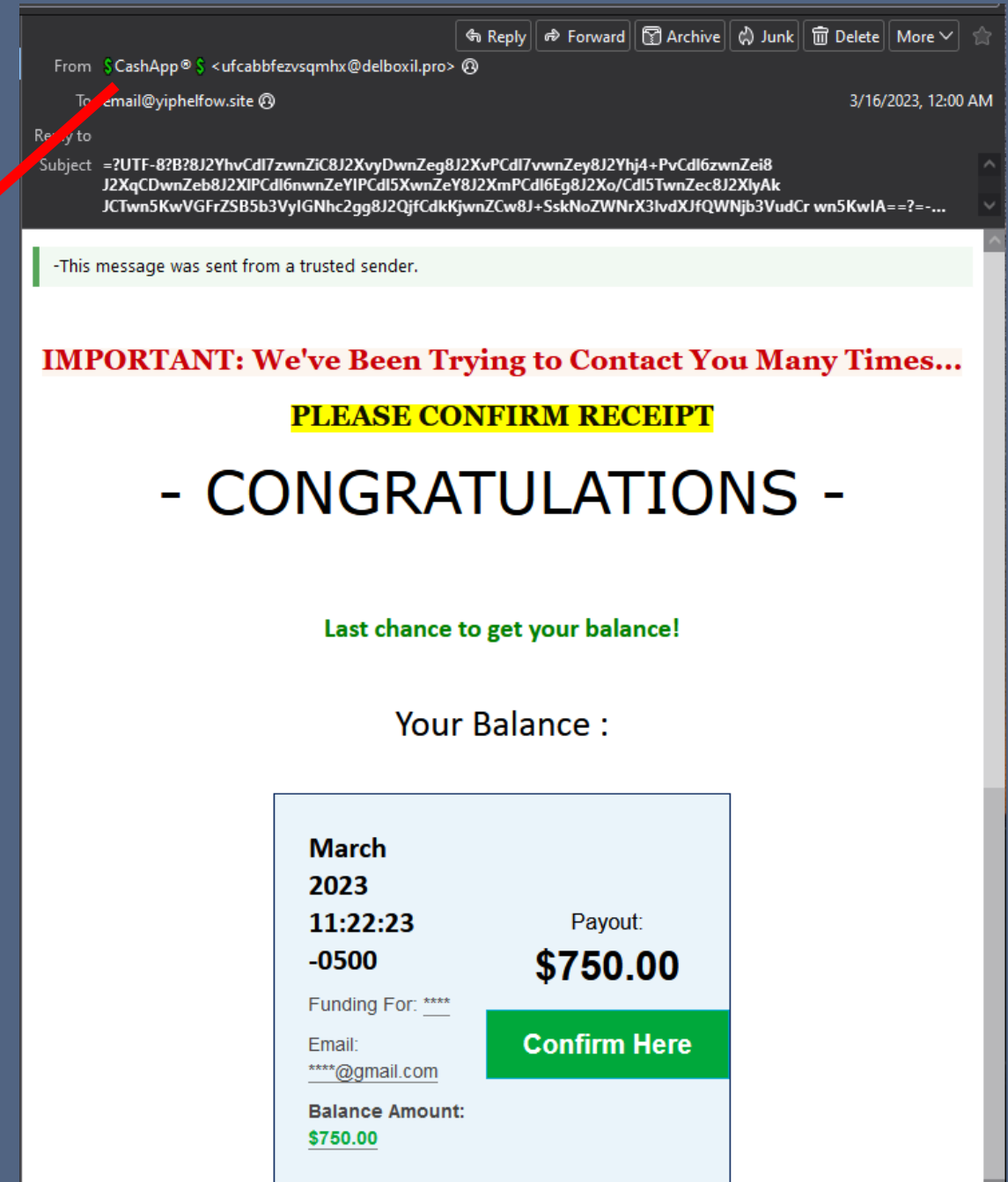
Email Phishing

From:
\$CashApp\$ <ufcabbfezvsqmhx@delboxil.pro>

Display Name

Email Address

Thunderbird email client



The screenshot shows an email interface with the following details:

- From:** \$CashApp\$ <ufcabbfezvsqmhx@delboxil.pro>
- To:** email@yiphelpow.site
- Subject:** =?UTF-8?B?8J2YhvCdI7zwnZiC8J2XvyDwnZeg8J2XvPCdl7vwnZey8J2Yhj4+PvCdI6zwnZei8J2XqCDwnZeb8J2XIPCdl6nwnZeYIPcdI5XwnZeY8J2XmPCdl6Eg8J2Xo/Cdl5TwnZec8J2XlyAkJCTwn5KwVGFzSB5b3VylGNhc2gg8J2QjfCdkJwnZCw8J+SskNoZWNrX3lvdXJfQWNjb3VudCrwn5KwIA==?=-...
- Date:** 3/16/2023, 12:00 AM

The email body contains the following text:

-This message was sent from a trusted sender.

IMPORTANT: We've Been Trying to Contact You Many Times...

PLEASE CONFIRM RECEIPT

- CONGRATULATIONS -

Last chance to get your balance!

Your Balance :

March	
2023	
11:22:23	Payout:
-0500	\$750.00
Funding For: ****	
Email: ****@gmail.com	Confirm Here
Balance Amount: \$750.00	

Email Phishing

From:
CVS <e3.vaston.info>

↑ ↑

Display Name Email Address

Thunderbird email client

From: CVS <contact@e3.vastoni.info> Reply Forward Archive Junk Delete More ☆

To: Al Williams 8:27 AM

Subject: atwms - we have been trying to reach you please respond

Special Offer!

Congratulations!

You've been selected to receive an **EXCLUSIVE OFFER!**

Complete this short 30-second survey about your experiences with

CVS PHARMACY

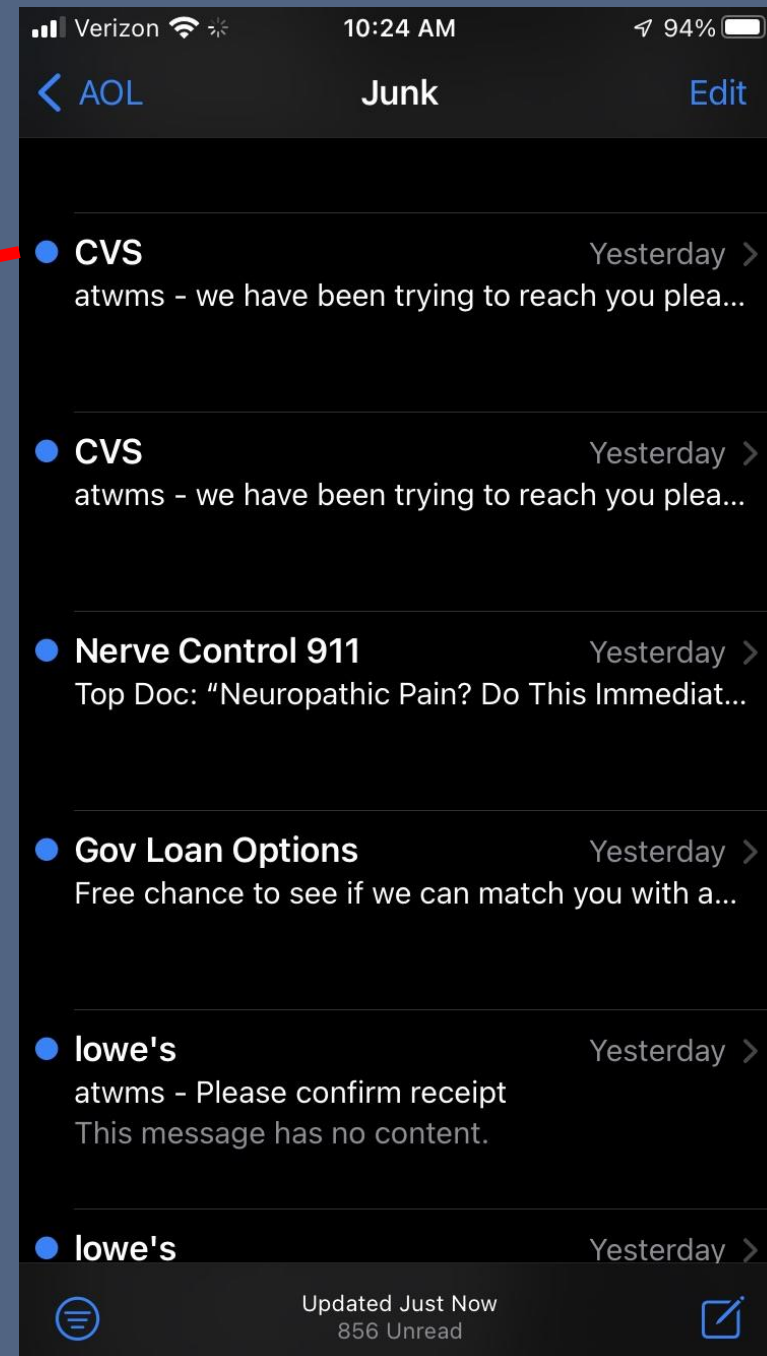
and receive your exclusive reward offer for participating.

Start Now

If you no longer wish to receive these emails, you may unsubscribe by clicking here or by writing to 9101 W. Sahara Ave, Las Vegas, NV 89117

Email Phishing

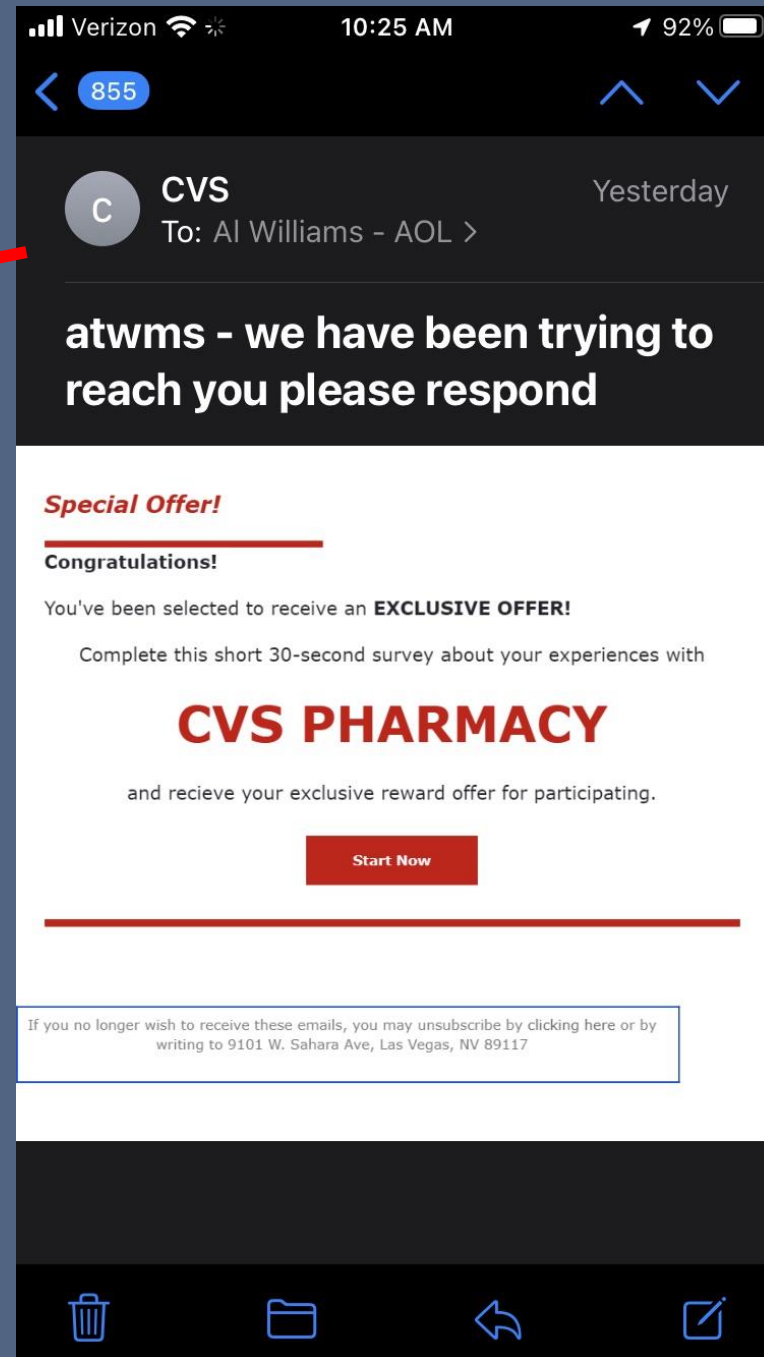
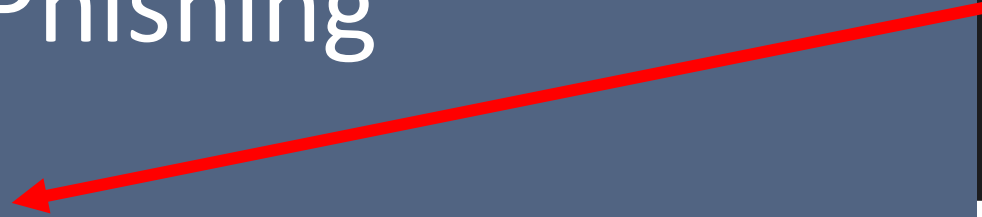
From: CVS



Mail for iOS email client

Email Phishing

From: CVS



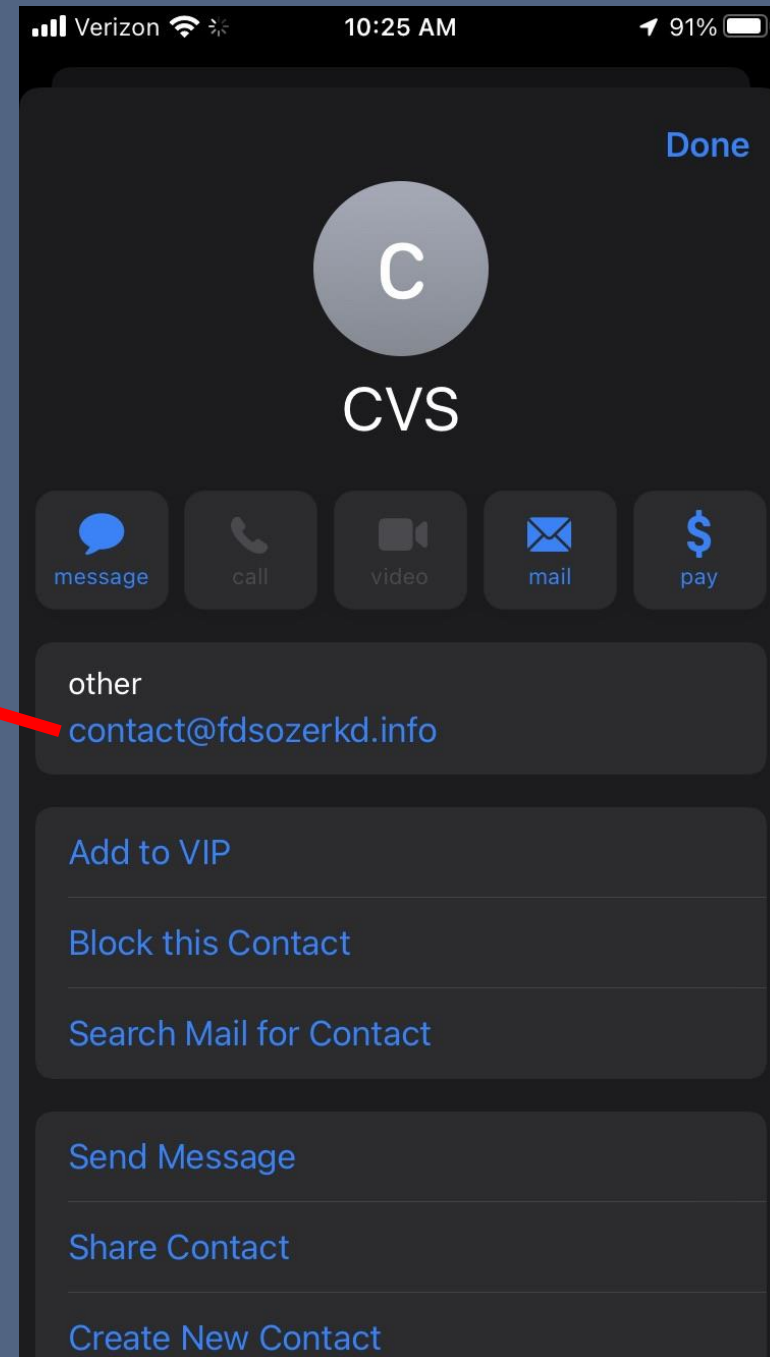
Mail for iOS email client

Email Phishing

From: CVS
<contact@fdsozerkd.info>

Tap the From address twice,
then long press the address to
open the screen to the right.

Mail for iOS email client



Email Phishing

Verify the From address

Don't click on any link in the email unless you are absolutely certain that you know the person or organization that sent the email.

If in doubt, use documents that you've received from that person or organization previously and call to verify that they sent the email.

Email Phishing - Links

Hovering the mouse over the link may show the actual link address. For example:

<https://www.ripoff.info>

instead of

<https://www.paypal.com>

Email Phishing - Links



ProtonMail offers Link Confirmation. On by default.

Email Phishing

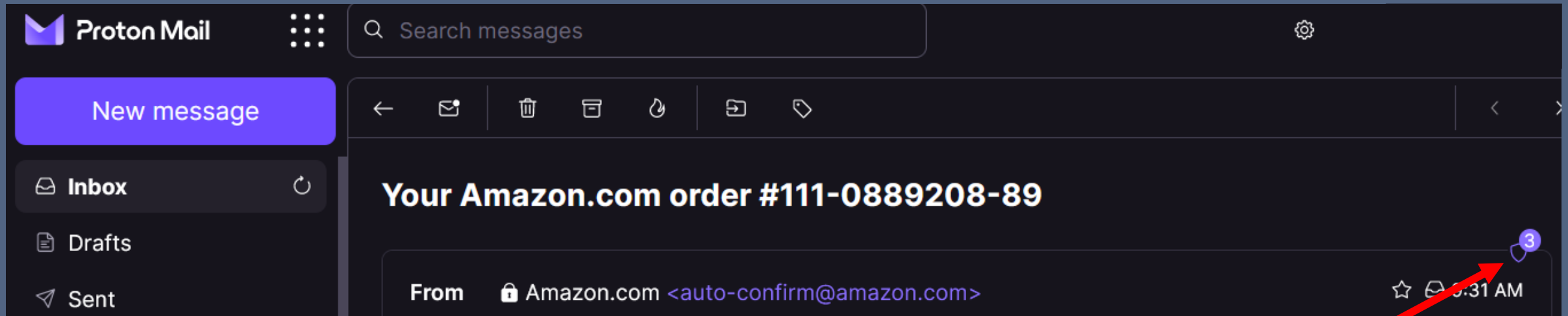
It will become harder and harder to recognize a scam by looking at the body of the email

We'll need to carefully look at the actual From address

We'll need to be very careful with links in emails

Email – Tracking

Email Tracking



3 Email Trackers

ProtonMail provides information about email trackers

3 email trackers blocked ✕

Email trackers can violate your privacy. Proton found and blocked 3 trackers.
[Learn more](#)

Amazon.com 3 ^

https://www.amazon.com/gp/r.html?C=1GDZONJ9HF37K&K=2WAAFRE18DL6E&M=urn:rtn:msg:202303181331536596484c08404f9bb24e9b888260p0na&R=3FOZ69HPEA0KP&T=O&U=https%3A%2F%2Fimages-na.ssl-images-amazon.com%2Fimages%2FG%2F01%2Fnav%2Ftransparent.gif&H=3QTXVTJ3XZWZBLLOAWDTAIYQAZCA&ref_=pe_386300_440135490_opens

http://g-ec2.images-amazon.com/images/G/01/x-locale/cs/te/MagicPixel_V319790361_.png

https://www.amazon.com/gp/r.html?C=1GDZONJ9HF37K&K=2WAAFRE18DL6E&M=urn:rtn:msg:202303181331536596484c08404f9bb24e9b888260p0na&R=3FOZ69HPEA0KP&T=O&U=https%3A%2F%2Fimages-na.ssl-images-amazon.com%2Fimages%2FG%2F01%2Fnav%2Ftransparent.gif&H=3QTXVTJ3XZWZBLLOAWDTAIYQAZCA&ref_=pe_386300_440135490_opens

[Got it](#)

Email trackers are often included in newsletters and marketing material

An email tracker is a very small image included in the email

When the email is opened, the linked image is opened from a source server. The source server collects information about you.

Whether the email containing the tracker has been opened

Date and time of opening

Device (computer) type and operating system

In some cases, your IP address and geographic location

Email clients that block email trackers

ProtonMail – image blocking automatically enabled

Thunderbird email client blocks remote images by default – regardless of email provider (Gmail, AOL, etc). User may download embedded content on individual basis or allow any pictures from selected contacts

Mail for iOS, Mail for macOS, Gmail, and others have settings to block trackers but the developers frequently change the way to access settings. Use Google to find the latest information.

Text Messages - Phishing

Text Message

Dad, I plan to arrive Friday around 3pm.

Great! We're looking forward to seeing you, Amy.

Text Message Phishing

(wells_fargo) important message from
security department!
Login.-=>
vigourinfo.com/secure.well5farg0card.html

Text Message Phishing is also known as SMiShing

SMS: Short Message Service

Text message source: Social Engineering, The Science of Human Hacking, page 9

Text messages are sent using cell phone numbers or multi-digit numbers

It is very hard to know who sent a text message unless you recognize the phone number or the multi-digit number

Best advice: Do not click on any links in a text message, unless you are absolutely certain that you know who sent you the text.

Websites

Your computer is infected!

DO NOT TURN YOUR COMPUTER OFF!

CALL 8xx-xxx-xxxx NOW!

Browsers have User-Agent

Chrome, Firefox, Safari, Brave, and others

The User-Agent provides information the website needs about our computer including the type of operating system we're using

- iOS

- iPadOS

- Linux (including type of Linux)

- Windows

Authoritative

The screen may mention Microsoft

The screen may mention Windows Defender

The scammer will try to convince you that an organization or app with authority is telling you what to do

Urgent

The screen message will urge you to act now

There may also be a voice telling you to act now

The scammer will try to use your emotions to cause you to act immediately

Unable to use your computer

None of the keyboard keys will do anything

This called browser lock

The scammer will try to convince your computer is unusable and that your only choice is to call them

What to do

1. Hold down the power button to turn your computer off
2. Wait 10 seconds
3. Turn the computer back on
4. If the browser locks again, repeat Steps 1 through 3
5. If the browser ask you if you want to restore your session, decline

If you call the scammer

They will ask for your credit card and will use it

They will ask you to help them install “monitoring” software on your computer

If you call the scammer

The “monitoring” software is remote desktop software

The software allows the scammer to work on your computer without your knowledge

What to do if you called the scammer

Check your Downloads folder for software downloaded the day you allowed the scammer to access your computer

Uninstall that downloaded software.

If you need help, there's a list of volunteers on Information Central

Protecting Us – Browser Lock

What to do to protect your computer

Continue to use Malwarebytes Premium

Add the free Malwarebytes Browser Guard extension to your Firefox or Chrome browser – stops tech support scams

<https://www.malwarebytes.com/browserguard>

If you need help, there's a list of volunteers on Information Central

Part 2
Scammers –
Scamming Our Online Accounts

June 1, 2pm, Cultural Center Theater

Part 3 – Invasive Species

July – date, time and location TBD

Questions?