



WBASNY
WOMEN'S BAR ASSOCIATION
of the STATE OF NEW YORK

Nota
by M&T Bank

Presents

Avoiding Financial Fraud and Scams at Your Law Firm

April 8, 2024
12:00 pm – 1:00 pm

Presenters:

Nicholas Beardi
Christopher Brescia
Amy B. Goldsmith, Esq.

Sponsored by

Nota
by M&T Bank

Ethical Responsibilities



Attorney Trust Accounts: the basics

What is IOLA?

Do you know?

1 – only for client funds and only in a bank located in NY

2 – no ATM withdrawals

Who are the permitted signatories? What are their responsibilities?

Are others authorized to take action?

22 NYCRR Part 1200 (Rule 1.15)



NEW YORK RULES OF PROFESSIONAL CONDUCT

Effective April 1, 2009

As amended through June 10, 2022

With Comments as amended through June 18, 2022

RULE 1.15:

**PRESERVING IDENTITY OF FUNDS AND PROPERTY OF OTHERS; FIDUCIARY
RESPONSIBILITY; COMMINGLING AND MISAPPROPRIATION OF CLIENT FUNDS
OR PROPERTY; MAINTENANCE OF BANK ACCOUNTS; RECORD KEEPING;
EXAMINATION OF RECORDS**

Image by [Mohamed Hassan](#) from [Pixabay](#)



**RULE 1.16:
DECLINING OR TERMINATING REPRESENTATION**

(c) Except as stated in paragraph (d), a lawyer may withdraw from representing a client when:

- (1) withdrawal can be accomplished without material adverse effect on the interests of the client;**
- (2) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is criminal or fraudulent;**
- (3) the client has used the lawyer's services to perpetrate a crime or fraud;**
- (4) the client insists upon taking action with which the lawyer has a fundamental disagreement;**
- (5) the client deliberately disregards an agreement or obligation to the lawyer as to expenses or fees;**

(13) the client insists that the lawyer pursue a course of conduct which is illegal or prohibited under these Rules.

(d) If permission for withdrawal from employment is required by the rules of a tribunal, a lawyer shall not withdraw from employment in a matter before that tribunal without its permission. When ordered to do so by a tribunal, a lawyer shall continue representation notwithstanding good cause for terminating the representation.



COMMITTEE REPORTS

**Opinion 2023-1: Ethical Obligations of
Lawyers and Law Firms Relating to
Attorney Departures**

Date

June 30, 2023



New York County Lawyers Association

Committee on Professional Ethics

Formal Opinion 751

<https://www.nycla.org/resource/ethics-opinion/new-york-county-lawyers-association-professional-ethics-committee-formal-opinion-751/>
September 20, 2017

Dishonest Employees

Unfortunately, even law firms are at risk for embezzlement at the hands of dishonest employees.

When bringing new team members on board, it is crucial to thoroughly screen each candidate, and be on the lookout for red flags and warning signs, such as:

- History of frequent job changes
- Recent or frequent relocations
- A history of criminal activity
- Substance abuse
- Living outside of their means
- Financial issues
- Significant debt
- Gambling habit



Nota
The M&T Bank

Tarter
Krinsky
& Drogin



Wire Fraud Scams

- Typically, social engineering is used to transfer funds to an unauthorized recipient.
- A cybercriminal may imitate a colleague or client that the victim (ie you, your assistant, your receptionist) may know and use that person's email address to get the victim to wire money to the criminal's bank account.

Social engineering is the art of manipulating people so they give up confidential information such as passwords, account numbers, credit card numbers.



Check Scams

Check scams continue to plague law firms across the country. As technology continues to evolve, it has become increasingly difficult to identify phony checks. Here are a few ways to verify whether a check is authentic and valid:



Consider Credit Cards/ACH

Get a Counterfeit Money Pen!



Ensure that the check was issued by a reputable bank



Check the microprinting on the signature line

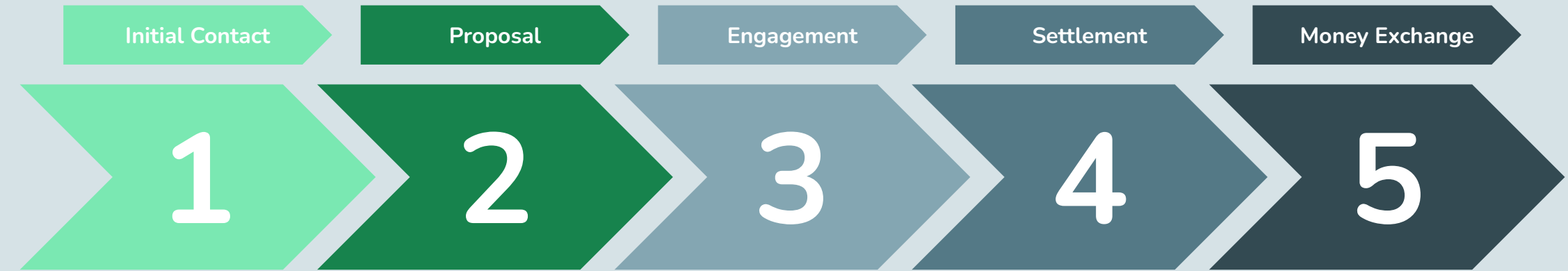


Be sure that the back of the check reads "original document"



Check for discoloration or ink smudging that could indicate that the check was tampered with

Typical Check & Wire Scam Scheme



Attorney receives email from an individual requesting assistance with an urgent transactional or litigation matter; generally located abroad (but not always!), counterparty or adversary is usually located in the attorney's jurisdiction.

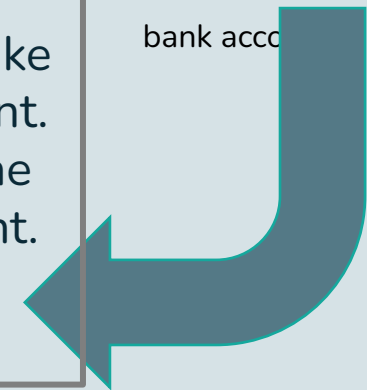
Email sender (the scammer) proposes a contingency fee. Writes that he is confident that matter will settle or close quickly. Attorney takes the case.

Attorney sends engagement letter, the scammer swiftly executes it.

Soon scammer notifies the attorney that the transaction has been consummated or the litigation has settled.

Attorney quickly receives the check and deposits it. The scammer requests an immediate wire distribution of the settlement funds. Lawyer retains the fee and wires the balance to a foreign bank account.

A bank may “clear” a check and make the funds available before the bank actually collects the funds. The bank may take weeks or even months to discover that the check is fraudulent. When that happens, the bank will notify the attorney that the check was fraudulent and the attorney must fund the account. (Many banks do not place “holds” on funds deposited into attorney trust accounts.)



Tips To Avoid Being Scammed



Confirm the Client

Seek additional information on the potential client and referral (if given) - verify the accuracy and genuineness of information contained in the solicitation, including phone numbers, addresses, websites, social, etc. To the extent possible, references should be obtained and researched thoroughly.

Comply with Rules

Retainer agreements should contain all of the terms specified by local statutes; the agreement should include all confirmed and pertinent information: valid billing street address, and as much contact information as possible. If the purported client is a corporate entity, an authorizing resolution of the shareholders or board of directors of the entity should be requested. Do not fear requiring a more substantial than-usual advanced fee deposit.

Take Your Time and Over-Communicate

Make clear to the prospective client that no attorney-client or other relationship has been created and no services shall be performed until (a) the lawyer has completed the engagement process in accordance with his/her firm's policies, (b) the lawyer receives confirmation from his/her bank that the advance fee deposit check or wire transfer has cleared in accordance with bank policy, and (c) the lawyer has accepted the representation.

Wait for the All Clear

All funds deposited into the trust account should be held until the bank confirms that payment of such funds has been honored by the payor bank.

Cautionary Signs

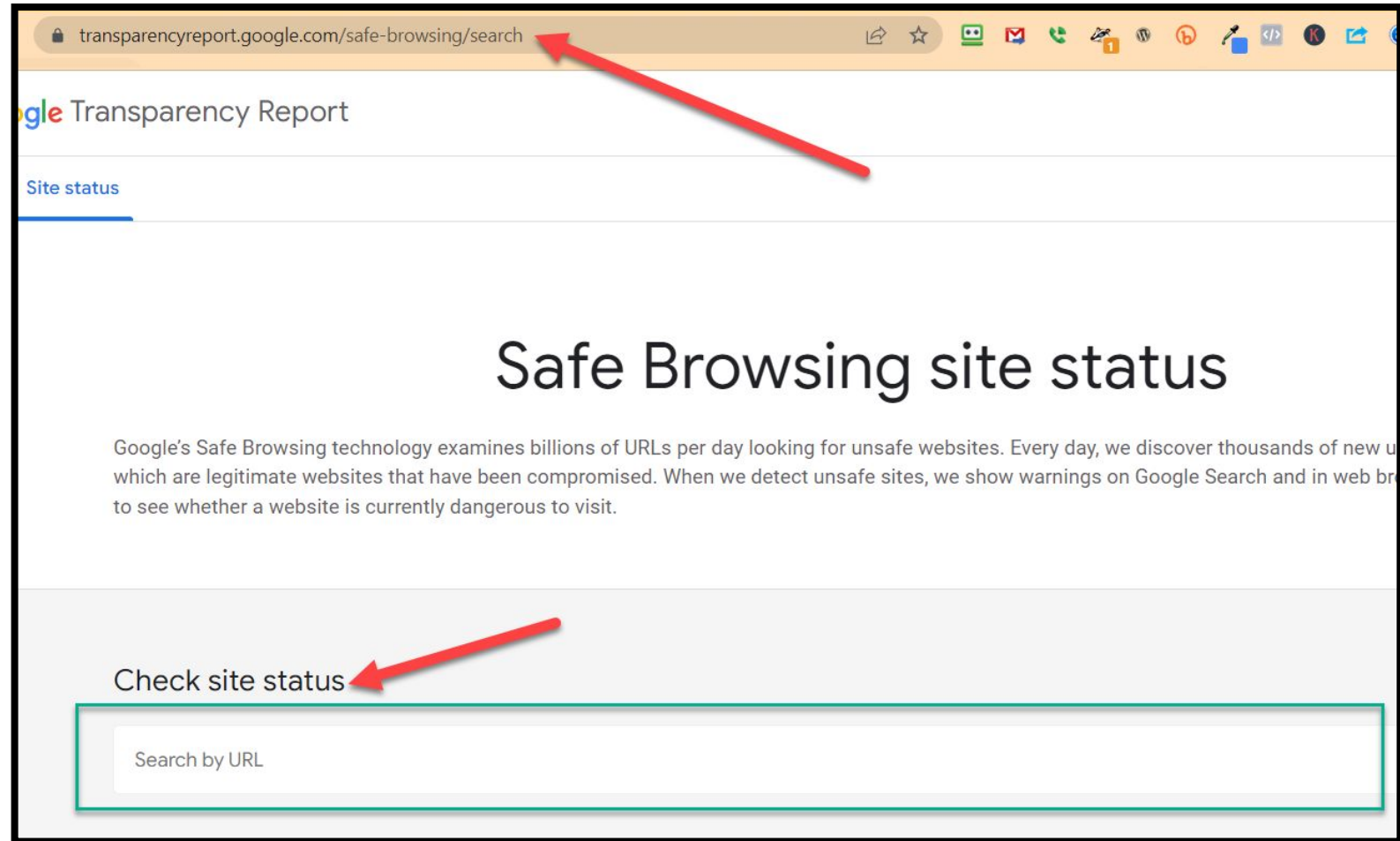
- Sender does not provide a referral source; says they found them via an online search.
- A salutation such as “Dear barrister/solicitor/counselor.”
- Email uses awkward phrasing or poor grammar (may be expected from a foreign contact).
- Email is sent to “undisclosed recipients” – the attorney is BCC’d.
- May seek counsel on a legal matter in an area of law the recipient attorney does not practice.
- Sender suggests that for this matter the attorney accept a contingency fee arrangement, even though that might not be customary for the attorney’s practice.
- Sender is quick to sign a retainer agreement, without negotiating.
- Sender assures the attorney that the matter will resolve quickly.
- Counterparty, if there is one, will also likely respond quickly.
- Sender insists that his funds must be wired to a foreign bank account (not always! But maybe a bank the attorney is not familiar with, in another state or region).



How To Mitigate Risk



Link Checking Sites



- <https://transparencyreport.google.com/safe-browsing/search>
- <https://scanurl.net/>
- <https://www.phishtank.com/>

Check site status

<https://storage.googleapis.com/zxvbsr00l2td00.appspot.com/1/files/s/pub/h/0/fileK5GtMYdVrnoJ.html?d=795243898423207875>

Current status

Some pages on this site are unsafe

The site <https://storage.googleapis.com/zxvbsr00l2td00.appspot.com/1/files/s/pub/h/0/fileK5GtMYdVrnoJ.html?d=795243898423207875> contains harmful content, including pages that:

- Try to trick visitors into sharing personal info or downloading software

Unsafe content might only appear on some pages of a website. Check the URL of the specific directory or webpage you want to visit for more safety info.

Client Portals: The Secret to Secure Communications

But how?

- They provide a platform with an enhanced level of security for storing and exchanging sensitive information and files
- They provide end-to-end encryption
- You AND your clients can activate 2FA
- They can provide clients with an enhanced level of security for making payments

Reduce phone calls, text and emails with clients

These are the three most common, yet least secure, methods of communication

Payment Protection Service from M&T Bank

TO MITIGATE CHECK FRAUD

- Positive Pay is \$40 a month per account +.08 per truncated check and \$3.00 per returned check. For this service you would submit a check ledger file before issuing checks. We then match any clearing checks to these files.
- Reverse Positive Pay is \$40 a month per account +.08 per truncated check and \$3.00 per returned check. For this service we simply report all checks attempting to clear. You would be responsible for reviewing these and selecting them to either pay or be returned.
- Payee Positive Pay is \$70 a month per account +.10 per truncated check and \$3.00 per returned check. For this service you would be responsible for uploading a check issue file before distributing checks. This file would include check date, dollar amount, check number and payee information. The bank would then review all clearing checks against this ledger and report any suspect items for you to decision.

TO MITIGATE ELECTRONIC DEBIT/ ACH FRAUD:

ACH Monitor is \$35 a month per account. For this service we simply report all debits attempting to clear. You would be responsible for reviewing these and selecting them to either pay or be returned. We are able to help you put authorized companies on file so they are not rejected.



PHISHING, WIRE FRAUD, & MALWARE

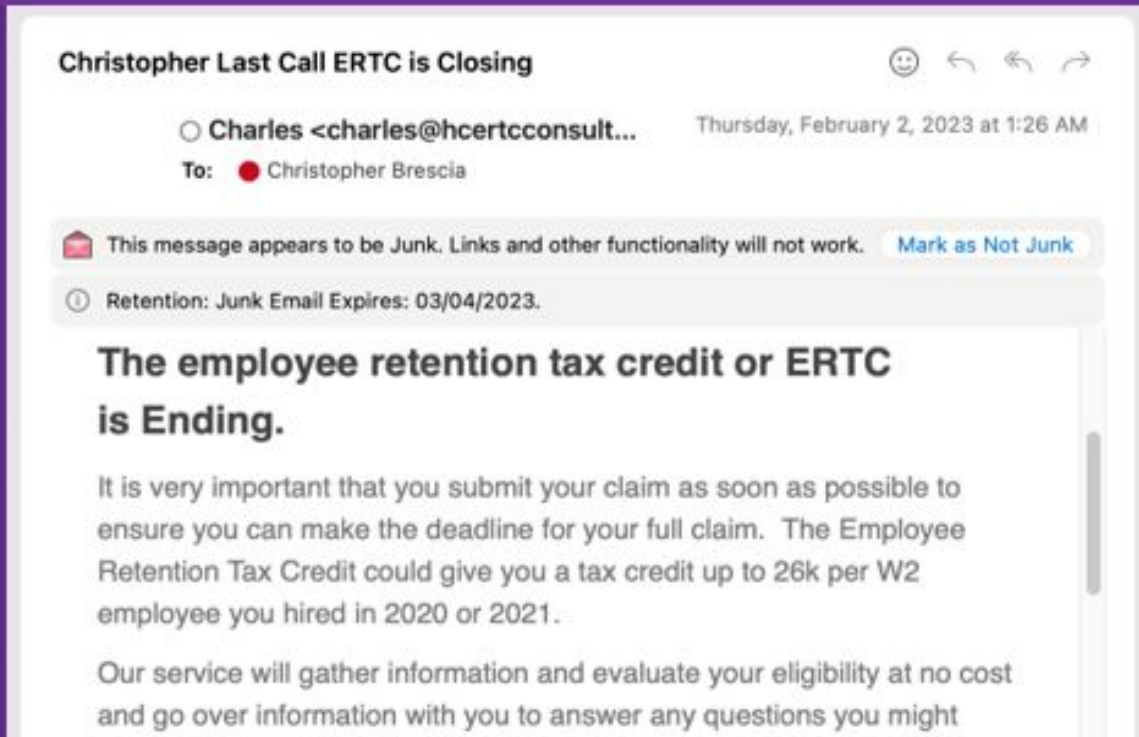
What they are

How they work

How you can defend against them

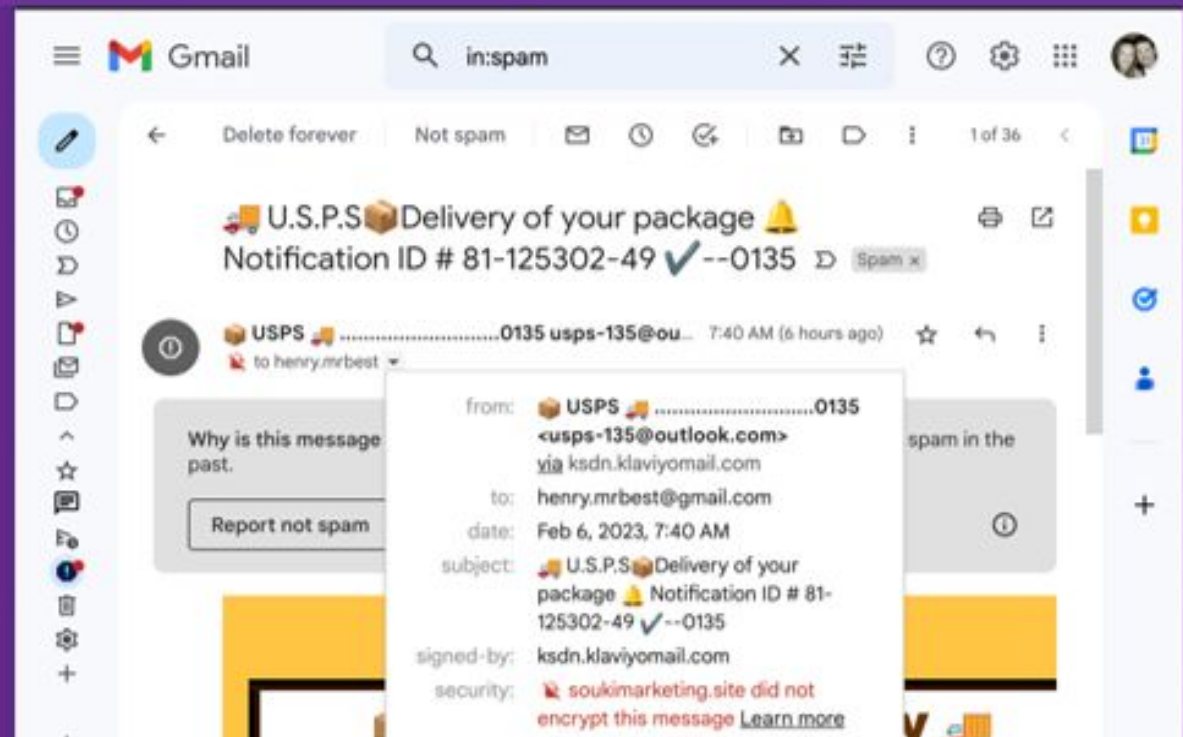
SPAM

Not lying, just not wanted.



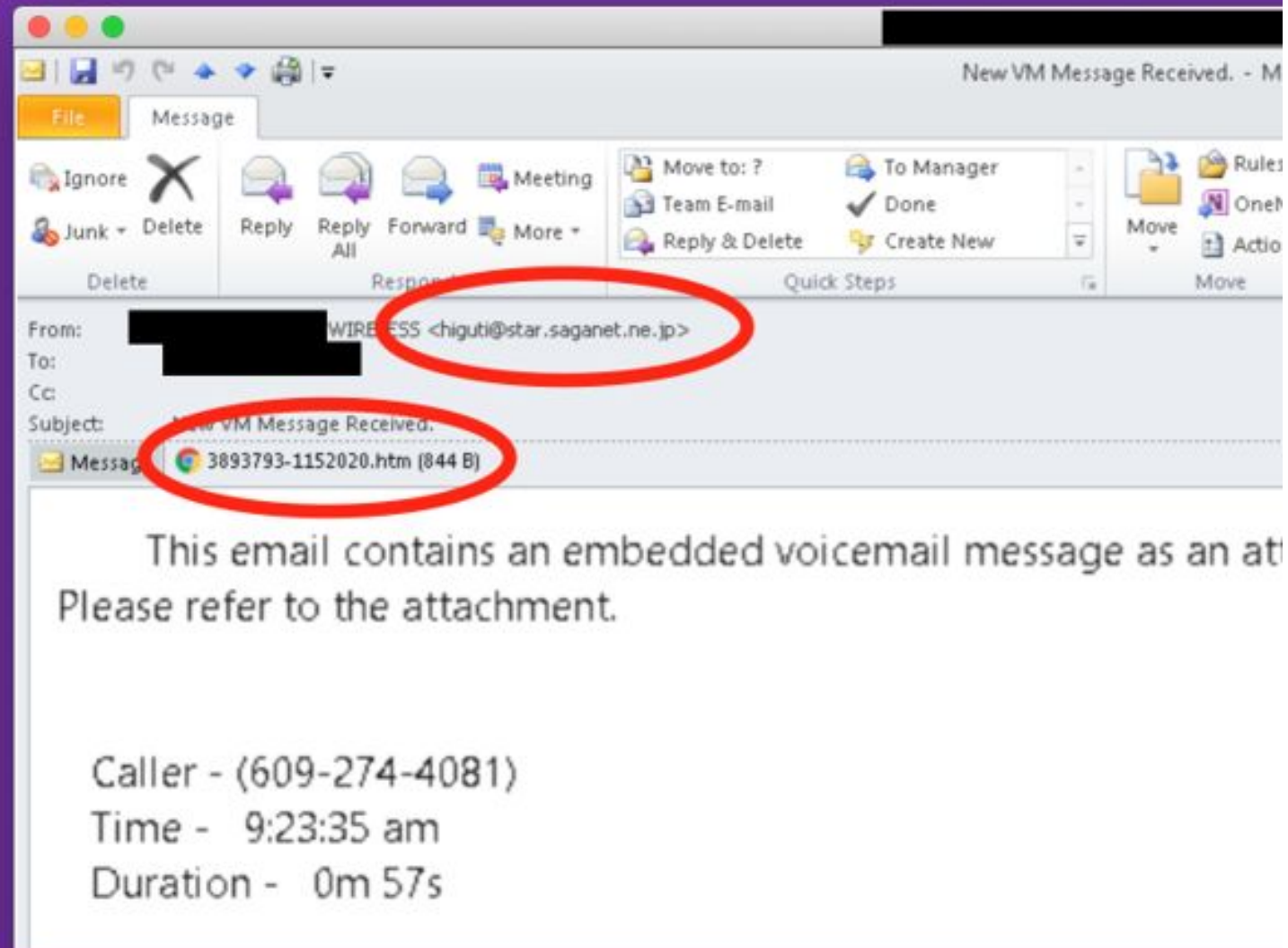
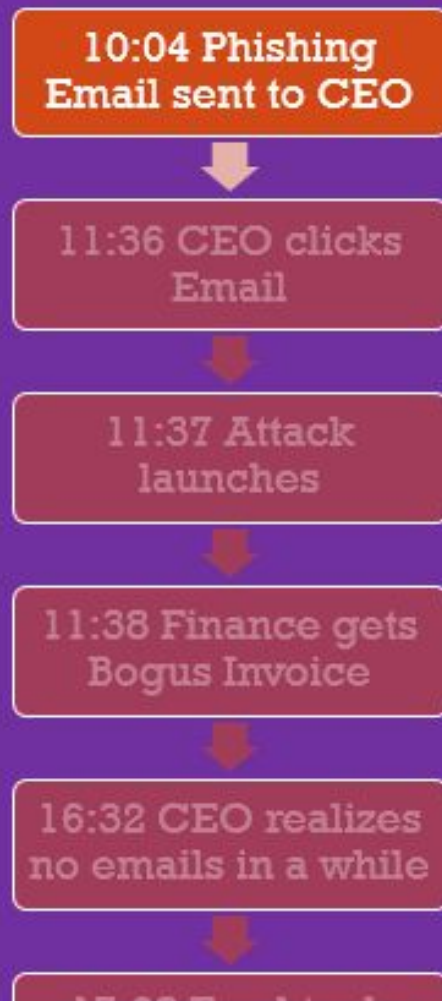
PHISHING

Lying about who they are to trick you into doing something.



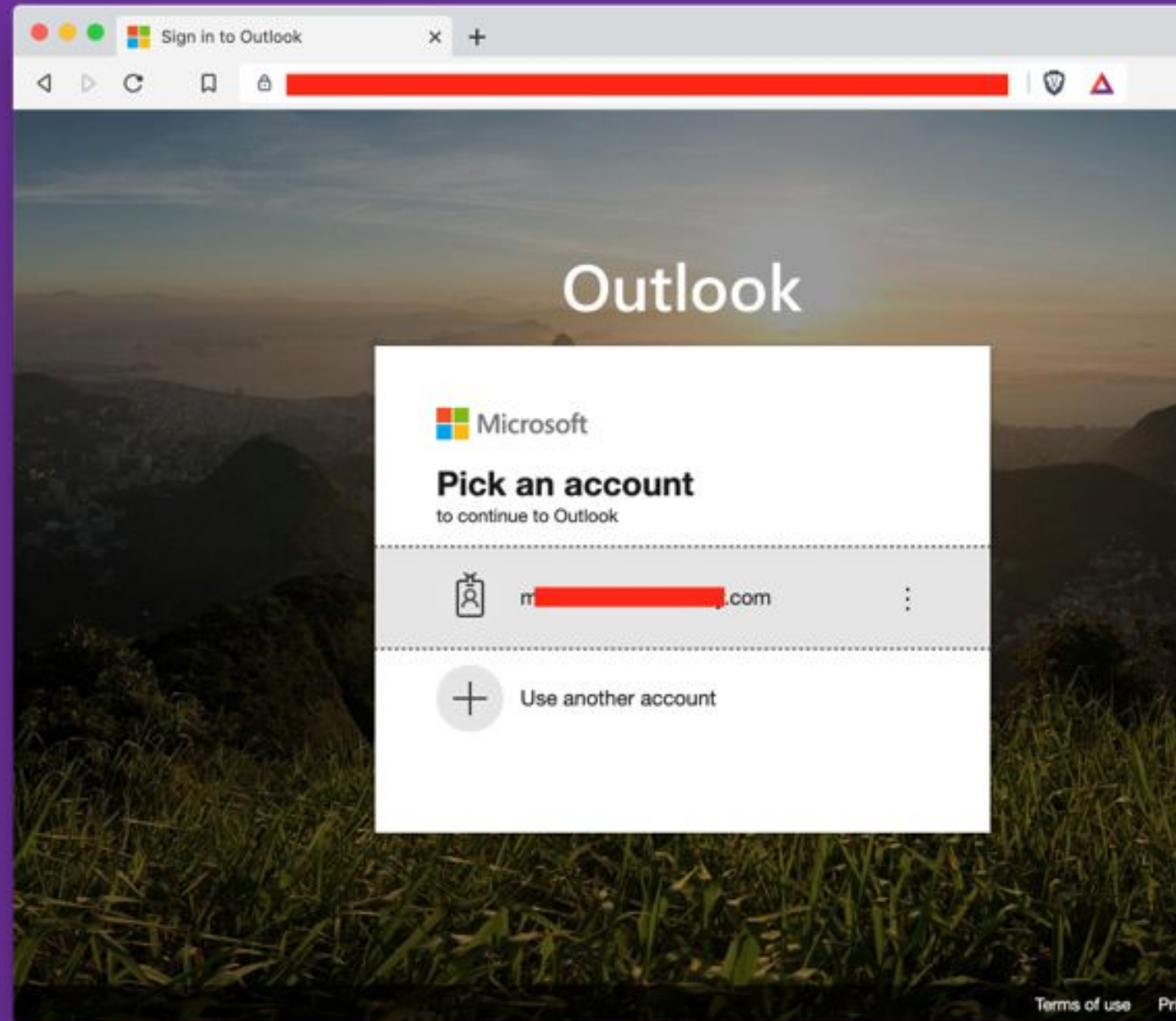
PHISHING

Lying, with intent.



PHISHING

Lying, with intent.



PHISHING

Lying, with intent.



Creates 'Rules' to delete all inbound email.

Scans email for Finance.

Create and Sends invoice.

Deletes evidence.

```
PS C:\WINDOWS\system32> Get-InboxRule -Mailbox [REDACTED] -Incl
Ms
-----
Junk E-mail Rule
..
where my name is not in the To box
Microsoft.Exchange.OOF.InternalSenders.Global
Microsoft.Exchange.OOF.AllExternalSenders.Global
has been sent out for signature to
[REDACTED].com
noreply@sf-notifications.com
[REDACTED]
sent only to me
Delegate Rule 2589944805102452737
noreply[REDACTED].com
MX Merchant Notification: Your payment was successful at [REDACTED]
eBay

PS C:\WINDOWS\system32>
```

PHISHING

Lying, with intent.



Actual Nickname

Sent from CEO's real account

From: [Redacted]
Sent: [Redacted] 11:38 AM
To: Jennifer [Redacted]
Subject: INVOICE # 10150

Jen,
Please arrange to pay the attached invoice today as this is long overdue and let me know once it has been processed. Payment is related to Professional services rendered to us. Thanks

[Redacted] President
[Redacted] (o)
[Redacted] (c)

[Redacted Signature]

"urgency"

nonsense

Real signature

PHISHING

Lying, with intent.

10:04 Malicious
Email sent to CEO

11:36 CEO clicks
Email

11:37 Attack
launches

11:38 Finance gets
Bogus Invoice

16:32 CEO realizes
no emails in a while

FROM:
Erica L Martinez LLC
1052 Monroe Street Houston TX 77002



BILL TO:


Real remittance
address

INVOICE #10150
DUE DATE 12/21/2019
DUE UPON RECEIPT

CLIENT PO
13383

USD

DESCRIPTION	AMOUNT
Professional Services Fee: For Research & Development Services Rendered for the months of :- (October - December 31st 2019)	78,623.00
TOTAL:	\$78,623.00

All Payments should be remitted via Wire Transfer or Ach Transfer to the banking details below:

Beneficiary Bank Name: BBVA COMPASS
Bank Address: 4112 College Hills Blvd San Angelo Tx 76904
Beneficiary Name: Erica L Martinez LLC
Account #: 677-903-9348
Routing #: 113010547

legit,
temporary
ACH account

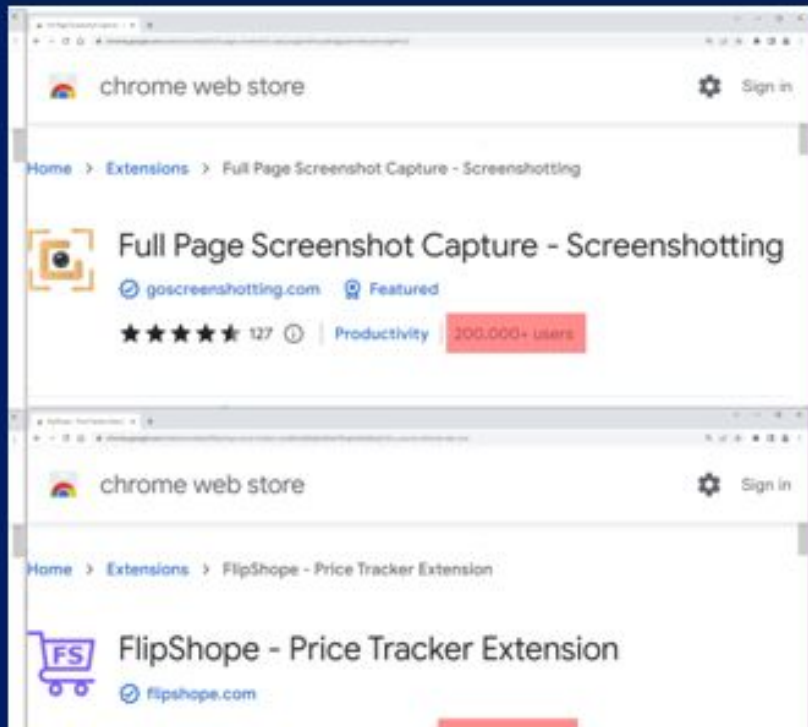
nonsense
signature
line



Admin Manager

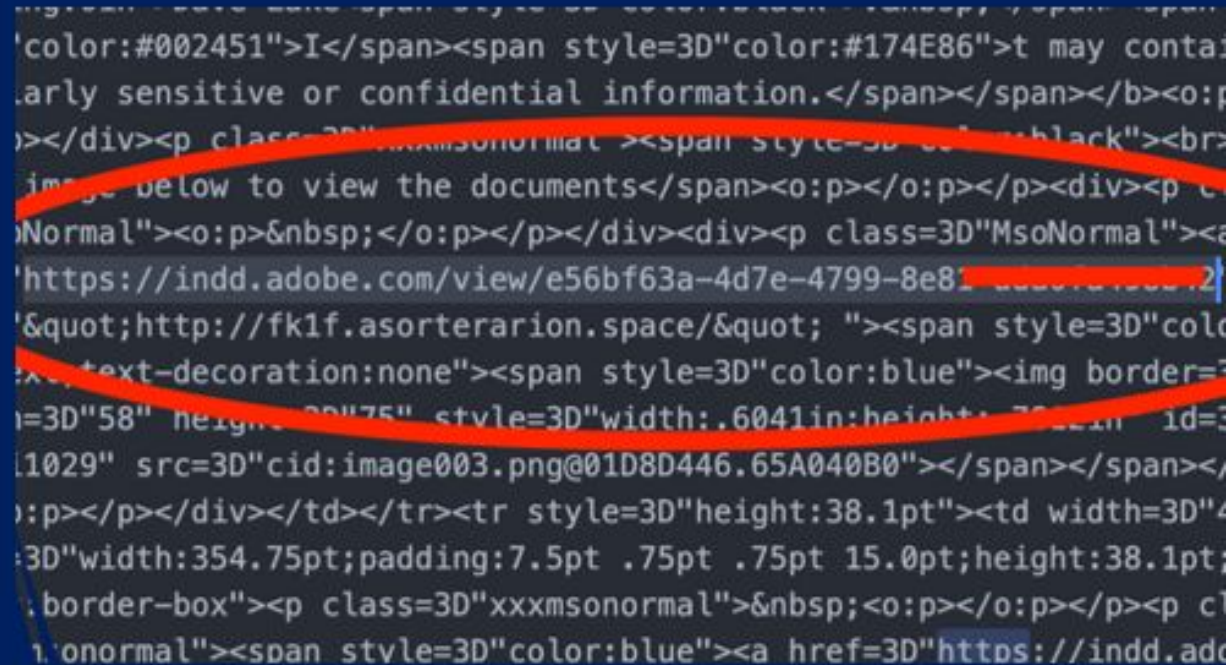
MALWARE

Any malicious program.



VIRUS

A type of Malware that inserts itself into other programs



MALWARE

Bad programs, bad guys.

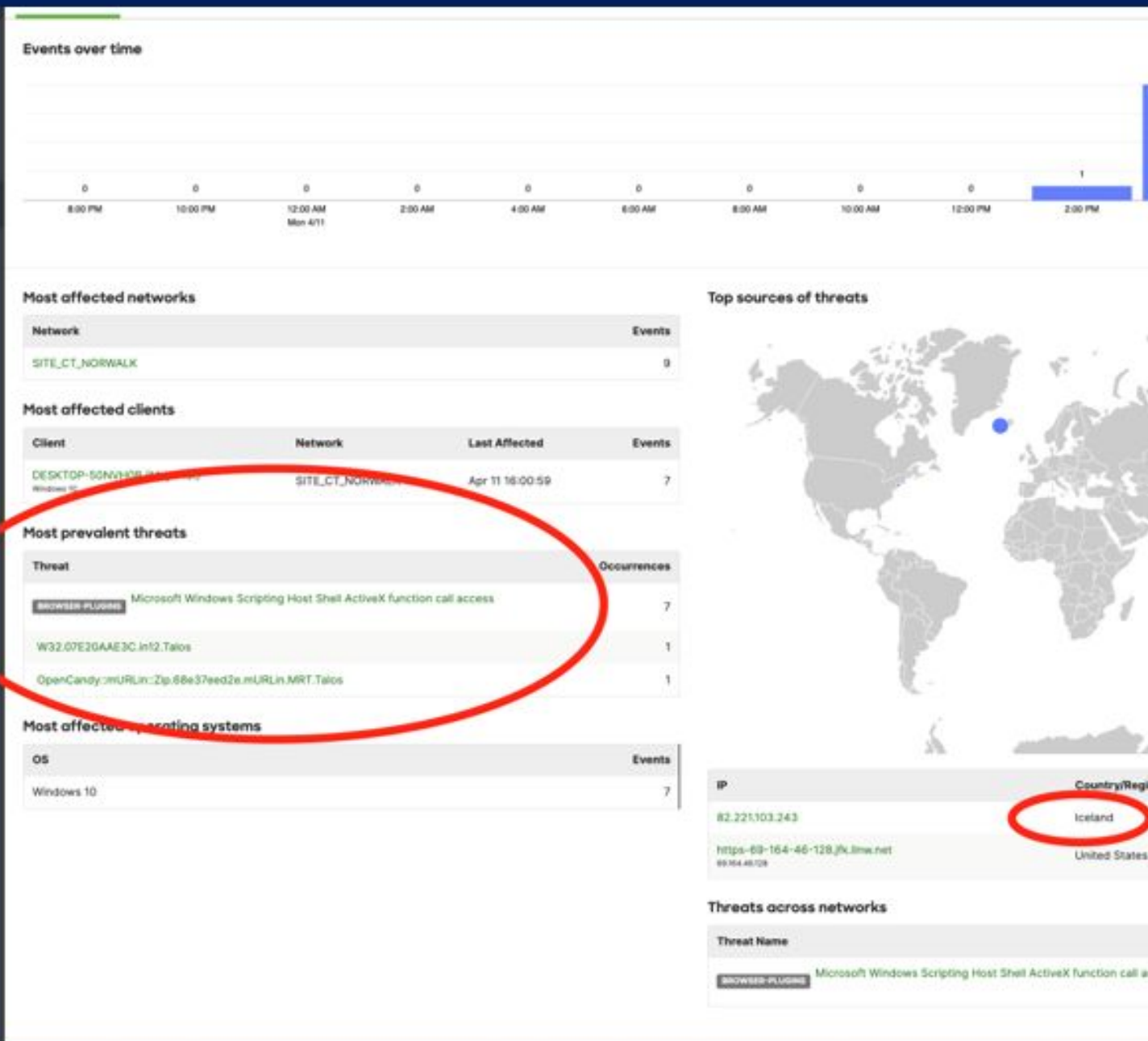
Suspicious Traffic
flagged on Firewall

Coming from a
Browser Extension

Trying to download
more malware

Payload from a
driver download

Payload included a
Trojan



MALWARE

Bad programs, bad guys.

Suspicious Traffic
flagged on Firewall

Coming from a
Browser Extension

Trying to download
more malware

Payload from a
driver download

Payload included a
Trojan

Security Center Apr 11

Search events

Filter

9 matching events

All times are in UTC

MX Summary **MX Events**

Time	Type	Source	Network	Destination	Disposition	Action	Details
Apr 11 16:00:59	File Scanned	download- lb.utorrent.com 82.221.103.243	SITE_CT_NORWA LK	DESKTOP-SONVH0B	Malicious	Blocke d	OpenCandy::mURLLin: ut/os/win10/track/stab
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 16:00:59	IDS Alert	82.221.103.243-80	SITE_CT_NORWA LK			Blocke d	BROWSER-PLUGINS
Apr 11 14:58:04	File Scanned	lsw.download3.utorrent. com 69.164.66.128	SITE_CT_NORWA LK		Malicious	Blocke d	W32.07E20AAE3C.in1 au=1&hash=0a776a75

MALWARE

Bad programs, bad guys.



Inspect packet

BROWSER-PLUGINS Microsoft Windows Scripting Host Shell
ActiveX function call access

Rule ID	Source	Destination	Action
1-8068	82.221.103.243:80	DESKTOP-50NVH0B (... Windows 10	Blocked

Offset	Hex	ASCII
00000000	38 d5 47 02 51 fb e0 cb bc 17 8c ee 08 00 45 00	18.G.Q.....E.l
00000010	05 dc 12 64 40 00 2f 06 b6 c6 52 dd 67 f3 c0 a8	l...d@./...R.g...l
00000020	01 79 00 50 d6 45 28 05 1e b3 44 08 1e c1 50 10	l.y.P.E(...D...P.l
00000030	00 ed 87 f0 00 00 62 65 6c 3a 68 79 64 72 61 2e	l.....bel:hydra.l
00000040	49 31 38 6e 2e 73 74 72 69 6e 67 46 72 6f 6d 54	l!18n.stringFromTi
00000050	70 6c 28 22 63 6f 6e 66 69 67 5f 6f 70 74 69 6f	lpl("config_optio
00000060	6e 73 5f 62 74 73 65 61 72 63 68 5f 66 69 6c 65	lns_btsearch_file
00000070	73 22 2c 7b 7d 29 7d 5d 2c 62 75 74 74 6f 6e 73	l s", ());],button
00000080	3a 5b 7b 74 69 74 6c 65 3a 68 79 64 72 61 2e 53	l: [[title:hydra.S
00000090	74 72 69 6e 67 73 2e 62 75 74 74 6f 6e 5f 62 61	l trings.button_bal
000000a0	63 6b 2c 67 6f 65 73 54 6f 3a 22 69 6e 73 74 61	l ick,goesTo:"instal
000000b0	6c 6c 5f 6f 70 74 69 6f 6e 73 22 2c 62 75 74 74	l ll_options",butt
000000c0	6f 6e 43 6c 61 73 73 3a 22 62 61 63 6b 22 7d 2c	l ionClass:"back"),l
000000d0	7b 74 69 74 6c 65 3a 68 79 64 72 61 2e 53 74 72	l l{title:hydra.Str
000000e0	69 6e 67 73 2e 62 75 74 74 6f 6e 5f 6e 65 78 74	l ings.button_nextl
000000f0	2c 67 6f 65 73 54 6f 3a 68 79 64 72 61 2e 67 65	l ,goesTo:hydra.gel
00000100	6e 65 72 61 74 65 47 6f 54 6f 28 22 63 6f 6e 66	l enerateGoTo("confi
00000110	69 67 5f 6f 70 74 69 6f 6e 73 22 2c 5b 22 66 69	l lig_options",["fil
00000120	6e 69 73 68 5f 69 6e 73 74 61 6c 6c 22 5d 2c 21	l inish_install"),l
00000130	30 29 2c 62 75 74 74 6f 6e 43 6c 61 73 73 3a 22	l l0),buttonClass:"l
00000140	6e 65 78 74 22 7d 5d 7d 29 7d 29 2c 6a 51 75 65	l lnext"))}}),JQue
00000150	72 79 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61	l iry(document).real
00000160	64 79 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61	l ldy(function){val
00000170	72 20 61 3d 68 79 64 72 61 2e 73 65 74 74 69 6e	l r a=hydra.settin
00000180	67 73 2e 67 65 74 28 22 6f 66 66 65 72 73 22 29	l lgs.get("offers")l
00000190	3b 69 66 28 61 29 66 6f 72 28 76 61 72 20 62 3d	l ;if(a)for(var b=l
000001a0	5f 2e 6b 65 79 73 28 61 29 2c 63 3d 30 3b 63 3c	l l_.keys(a),c=0;c<l
000001b0	62 2e 6c 65 6e 67 74 68 3b 63 2b 2b 29 68 79 64	l b.length;c++)hydl
000001c0	72 61 2e 61 76 61 69 6c 61 62 6c 65 4f 66 66 65	l ra.availableOffe
000001d0	72 73 5b 62 5b 63 5d 5d 26 26 28 68 79 64 72 61	l rs[b[c]]&&(hydra
000001e0	2e 61 76 61 69 6c 61 62 6c 65 4f 66 66 65 72 73	l l.availableOffers
000001f0	5b 62 5b 63 5d 5d 28 29 2c 68 79 64 72 61 2e 67	l l[b[c]](),hydra.g
00000200	65 6e 65 72 61 74 65 56 69 65 77 73 4f 72 64 65	l enerateViewsOrde
00000210	72 28 62 5b 63 5d 29 29 7d 29 2c 24 28 64 6f 63	l r(b[c]))},\$(docl
00000220	75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e	l ument).ready(fun
00000230	63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e	l ction){functionl
00000240	20 61 28 29 7b 68 79 64 72 61 2e 61 72 72 43 6f	l a(){hydra.arrCol
00000250	6d 6d 61 6e 64 73 2e 6c 65 6e 67 74 68 3e 3d 32	l lemands.length=2l
00000260	26 26 68 79 64 72 61 2e 61 72 72 43 6f 6d 6d 61	l l&&hydra.arrComm
00000270	6e 64 73 5b 31 5d 26 26 68 79 64 72 61 2e 49 6e	l nds[1]&&hydra.In
00000280	73 74 61 6c 6c 2e 64 6f 49 6e 73 74 61 6c 6c 28	l stall.doInstall(l

MALWARE

Bad programs, bad guys.



<input type="checkbox"/>	AppIntegratorStub64.dll	Malicious	Un
<input type="checkbox"/>	ARBITER.DLL	Malicious	Un
<input type="checkbox"/>	APPINTEGRATORSTUB.DLL	Malicious	Un
<input type="checkbox"/>	AppIntegrator64.exe	Malicious	Un
<input type="checkbox"/>	39SrcAs.dll	Malicious	Un
<input type="checkbox"/>	APPINTEGRATOR.EXE	Malicious	Un
<input type="checkbox"/>	39skin.dll	Malicious	Un
<input type="checkbox"/>	cbsidlm-cbsi188-KONICA_MINOLTA_magico...	Malicious	Un
<input type="checkbox"/>	39skin.dll	Malicious	Un

MALWARE

Bad programs, bad guys.



13 / 61

13 security vendors and no sandboxes flagged this file as malicious

68e37eed2e04830fce9f735d8a2eceb19a651394f5d590581370ac5d7754d90
install.1649724368.zip

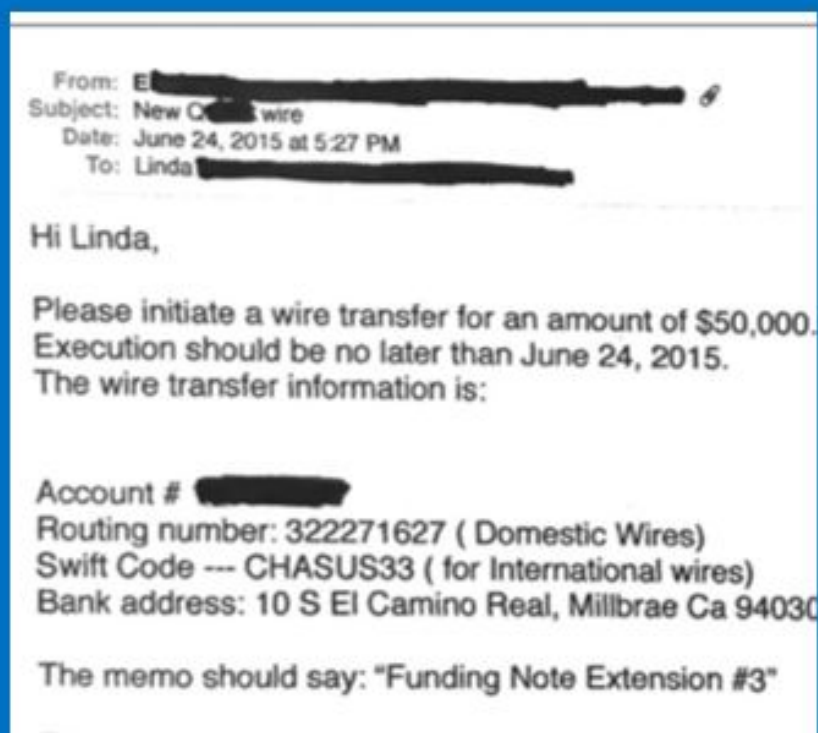
zip

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
CAT-QuickHeal		Script.Trojan.A2051064	
Cyren	Trojan.FIBN-3	Trojan.FIBN-3	
ESET-NOD32		Win32/OpenCandy.J Potentially Unsafe	
Gridinsoft		Adware.U.OpenCandy.oa	
McAfee-GW-Edition		Artemis	
TrendMicro		HEUR_HTMJS.D	
Yandex		Trojan.Etecer.bRUI2z.6	
Ad-Aware		Undetected	

WIRE FRAUD

Tricking a victim into sending funds to an attacker's account.



CRED. THEFT

Using stolen credentials to access accounts and transfer funds to an attacker's account.



WIRE FRAUD

1. Agent credentials stolen
2. Inbox monitored (via forwarding)
3. Closing Date entered in MLS
4. False Wiring Instructions sent to borrower
5. “Bank” calls to ‘verify’ wiring change
6. Money ends up in attacker’s accounts

From: John Smith <john@closing-disclosures4.com>

Date: Mon, May 01, 2021, 5:37 PM

To: Jane Smith <jane@janesmith.com>

Subject: 123 Louisiana St.

1

Check the sender’s email address to make sure it matches your mortgage company’s emails.

Hi Jane,

You just received your closing disclosure, congratulations!
Your wiring instructions are attached for cash to close on 123 Louisiana St.

Please process the payment and respond with proof of payment attached.

You will need a form of ID for the closing appointment.

Wire the funds as soon as possible with the attached wiring instructions to avoid any delays in processing.

Thank you,

John Smith

Escrow Officer

555 West First Street, Suite 5 San Diego, CA 92104

johnsmith@closingescrow.com

www.ClosingEscrow.com

2

Call your mortgage or escrow company directly to verify the email is legitimate. Don’t use the phone number in the email as this could connect you to a scammer.

NOTICE: The information contained in this message is proprietary and/or confidential and may be privileged. If you are not the intended recipient of this communication, you are hereby notified to: (i) delete the message and all copies; (ii) do not disclose, distribute or use the message in any manner; and (iii) notify the sender immediately.

HOW TO DEFEND YOUR ORGANIZATION

What they are

How they work

How you can defend against them

HOW TO DEFEND

chris@freshtech.it
(860) 768-9300 x200



Vet and Hire a Professional IT+Cyber Co.



Get Cyber Mature



Use MFA (2FA) everywhere



Use a Password Manager



Get a good Tech Stack



Get a Business-class Firewall



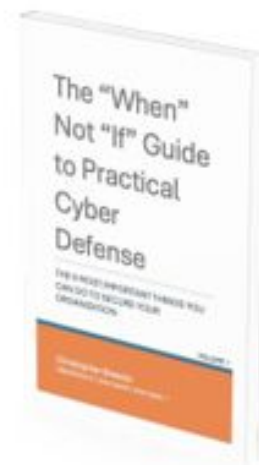
Develop and Test Incident Response Plans



Get Cyber Insurance



Train your people



HIRE PROFESSIONALS

Hire professionals and listen to them. You should not try to be the expert at IT / Cyber any more than I should try to be the expert at law.

Vet them as diligently and thoroughly as if you were hiring a new CEO.

Favor unlimited support (all-you-can-eat) models instead of break-fix.

chris@freshtech.it
(860) 768-9300 x200

**FRESH
TECH**



TRAIN YOUR PEOPLE

People, yourself included are the biggest risk to any organization.

1. Security Awareness Training
2. Acceptable Use Policy
3. Remote Work Policy
4. Password Policy
5. Incident Response Plans

chris@freshtech.it
(860) 768-9300 x200

FRESH
TECH

New Phishing Campaign

1. Scenario

2. Audience

3. Schedule

GoToMeeting

Featured

Coworker Meeting Invitation

In-progress meeting invite from random coworker.

Customize Preview

Select

employees.

Microsoft

Featured

Coworker Meeting Invitation

Teams meeting invite from random coworker.

Customize Preview

Select

Repayment

U.S. Treasury COVID-19 stimulus check repayment notification.

Customize Preview

Generic

Custom - Coronavirus disease (COVID-19) outbreak

Offices will be shutdown as a preventive measure notification.

Customize Preview

TRAIN YOUR CLIENTS

Someone's going to train them. It will either be you, or a thief.

1. Don't trust any info in email,
2. Always confirm details directly with your known point of contact
3. Urgency is deadly

chris@freshtech.it
(860) 768-9300 x200



PROTECT YOURSELF FROM WIRE FRAUD



You're finally buying your dream home. It's time to wire your closing costs to the title company. You follow the directions of an email that came to your inbox. Only, the email was fraudulent, and you just lost your hard-earned cash ... and the house of your dreams.

It's called wire fraud, and it's happening all around the country. Criminals comb through sites looking for pending home sales. Once identified, they will find contact information for the parties involved in the transaction. It's easy to do through public websites and online searches. Then, they hack into a real estate agent's or title company's email system, monitor communications, and, when the time is right, send a fraudulent email that looks like it's from

HOW CAN YOU AVOID BEING A VICTIM?

- 1. BE SKEPTICAL.** Beware of any changes in wiring instructions, like those that have you wire money to a company that is not the same name as the title company you're using.
- 2. ASK FOR PHONE CALLS.** Ask for all wire transfer instructions to be delivered to you via phone with the number listed on the title company's website. If you receive an email that details changes in the wire transfer instructions and that email contains a phone number, don't call it.
- 3. VERIFY ALL COMMUNICATIONS.** Call the title company immediately after you send any funds via wire transfer

5. LEARN TO SPOT A FRAUDULENT EMAIL.

There are telltale signs that an email is a fraud. Look for misspellings, poor grammar and mistakes in the content. Many times, the property address is spelled incorrectly, dollar figures are missing dollar signs, and the return email address doesn't match, or the company name is spelled incorrectly.

If you are a victim of a wire fraud crime in Florida, call the Attorney General's Fraud Hotline at (888) 966-7726. You should also file a complaint with the Federal Bureau of Investigation (FBI). To do so, contact the nearest FBI field office. Locations are listed at fbi.gov/contact-us/field-offices.

Sources: ahttle.com and Ray National

USE MULTI-FACTOR CODES

That 6-digit code makes you a slightly harder target than the next person (because they need to 'steal' your phone, too)

Do this EVERYWHERE

Resist the “don't ask again” temptation

Opt for code-based (versus yes/no) confirmation

chris@freshtech.it
(860) 768-9300 x200

FRESH
TECH



2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

 [REDACTED]@gmail.com ▾

2-Step Verification

A text message with a 6-digit verification code was just sent to [REDACTED]

G- Enter the code

KNOW YOUR INSURANCE

Credential theft and wire fraud are two different policy coverages.

Standalone policies are better than addendums.

Actions you take during a breach can invalidate your claim. Be sure to work with your carrier when building your Response Plans

chris@freshtech.it
(860) 768-9300 x200



USER TIER	Cyber Insurance Policy Coverage Comparison		
	\$250,000 Policy	\$500,000 Policy	\$1,000,000 Policy
LIMIT	\$250,000	\$500,000	\$1,000,000
RETENTION/DEDUCTIBLE	NONE	\$2,500	\$2,500
ENTERPRISE SECURITY EVENT CLAIM	\$250,000	\$500,000	\$1,000,000
PRIVACY REGULATION CLAIM	\$250,000	\$500,000	\$1,000,000
CRISIS MANAGEMENT EXPENSE	\$250,000	\$500,000	\$1,000,000
FRAUD RESPONSE EXPENSE	\$250,000	\$500,000	\$1,000,000
PUBLIC RELATIONS EXPENSE	\$250,000	\$500,000	\$1,000,000
FORENSIC AND LEGAL EXPENSE	\$250,000	\$500,000	\$1,000,000
MITIGATION EXPENSE	\$250,000	\$500,000	\$1,000,000
COMPUTER EXTORTION EXPENSE	\$10,000	\$500,000	\$500,000
PCI-DSS CLAIM	\$250,000	\$500,000	\$1,000,000
PCI RE-CERTIFICATION	INCLUDED	INCLUDED	INCLUDED
RANSOMWARE	\$10,000	\$100,000	\$1,000,000
SOCIAL ENGINEERING	\$10,000	\$100,000	\$100,000
TELECOM THEFT	\$10,000	\$100,000	\$100,000
BUSINESS INTERRUPTION AND DATA RECOVERY	NOT INCLUDED	\$500,000 6 HOUR WAITING PERIOD	\$1,000,000 6 HOUR WAITING PERIOD
E-THEFT EXPENSE	\$100,000	\$100,000	\$100,000
GDPR PRIVACY CLAIMS	\$250,000	\$500,000	\$1,000,000

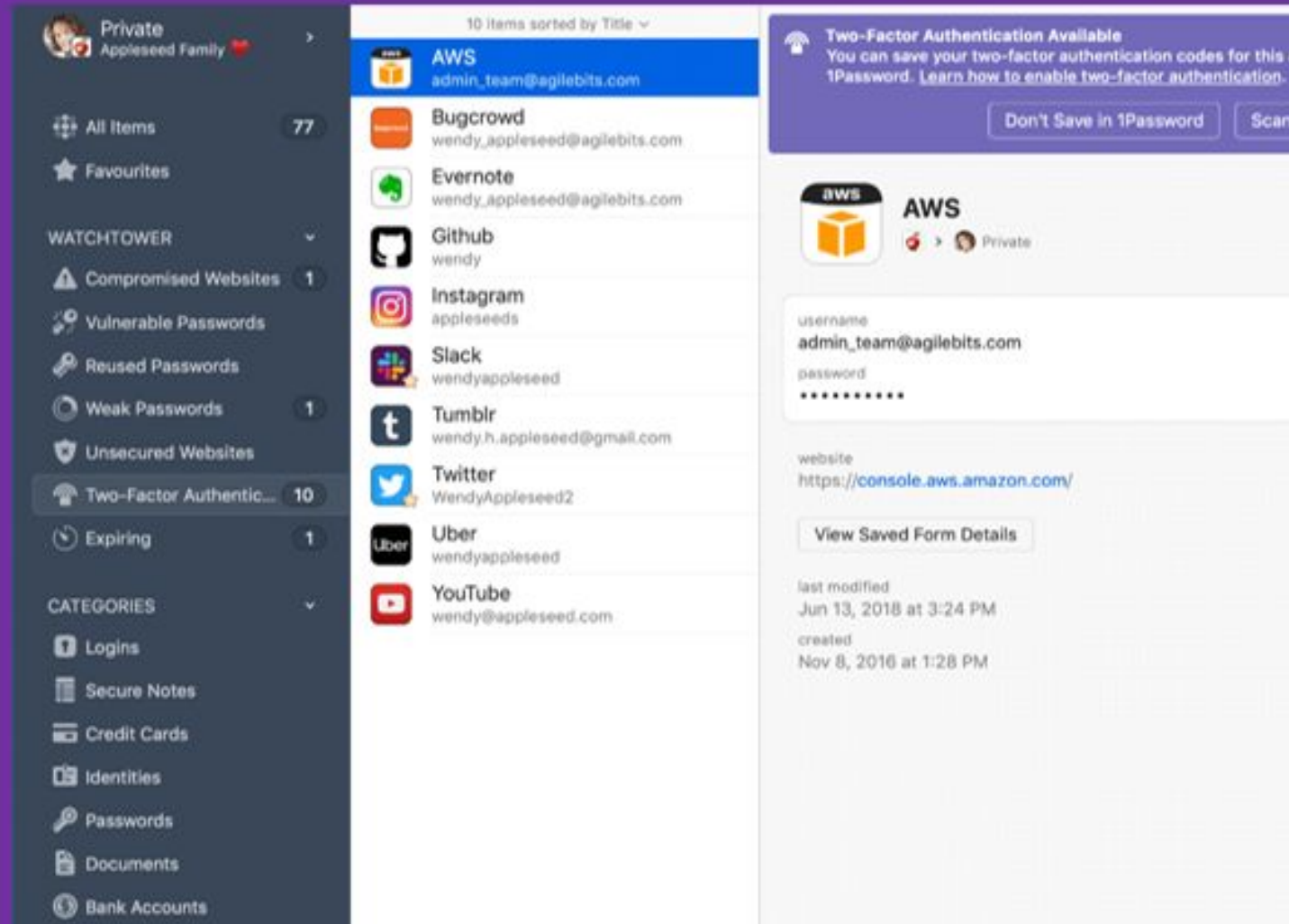
GET A PASSWORD MANAGER

Generates, stores, and tracks your passwords and sensitive information.

Keeper Security and 1Password.com are currently the only two we recommend for business or personal use.

Never use the same password twice.

chris@freshtech.it
(860) 768-9300 x200



GET WINDOWS DEFENDER

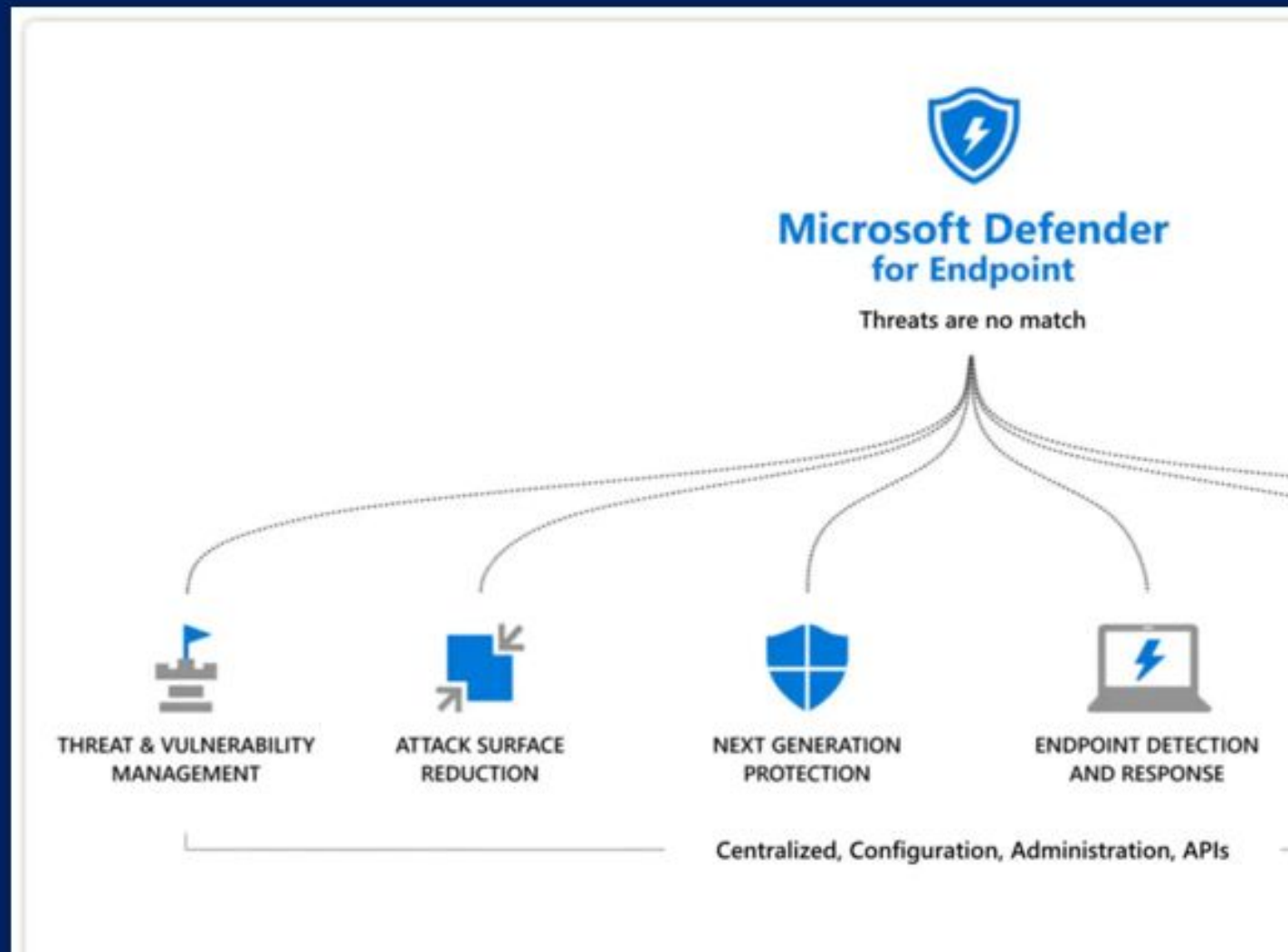
As the most-hacked operating system on the planet, **Microsoft Defender** has more field data than any other security company.

Get a professional IT Company to provide **SentinelOne** or another next-gen automatic recovery tool (EDR / MDR / XDR)

Stop using TrendMicro, Webroot, McAfee, Norton

chris@freshtech.it
(860) 768-9300 x200

**FRESH
TECH**



DONT TRUST EMAIL

Don't call numbers, Don't reply to emails, Don't use unsubscribe links, Don't click attachments or do anything else with suspicious emails.

Get info directly from known sources.

Bad emails can look legit!

chris@freshtech.it
(860) 768-9300 x200



From: John Smith <john@closing-disclosures4.com>
Date: Mon, May 01, 2021, 5:37 PM
To: Jane Smith <jane@janesmith.com>
Subject: 123 Louisiana St.

1

Check the sender's email address to make sure it matches your mortgage company's emails.

Hi Jane,

You just received your closing disclosure, congratulations!
Your wiring instructions are attached for cash to close on 123 Louisiana St.

Please process the payment and respond with proof of payment attached.

You will need a form of ID for the closing appointment.

Wire the funds as soon as possible with the attached wiring instructions to avoid any delays in processing.

Thank you,

John Smith

Escrow Officer

555 West First Street, Suite 5 San Diego, CA 92104

johnsmith@closingescrow.com

www.ClosingEscrow.com

2

Call your mortgage or escrow company directly to verify the email is legitimate. Don't use the phone number or email as this could connect you to a scammer.

NOTICE: The information contained in this message is proprietary and/or confidential and may be privileged. If you are not the intended recipient of this communication, you are hereby notified to: (i) delete the message and all copies; (ii) do not disclose, distribute or use the

IGNORE 'URGENCY'

Logic makes people THINK.
Emotion makes people ACT.

Phishing emails are 'scary' and
'urgent' on purpose. People get in
fight-or-flight and think first, ask
later.

chris@freshtech.it
(860) 768-9300 x200

FRESH
TECH

Urgent Request

Reply



Will Catt <calebangeluv80@gmail.com>

To ○ Jane North

Hello are you available?

Please I need your assistance urgently

Will Catt

Professor

Communication Sciences

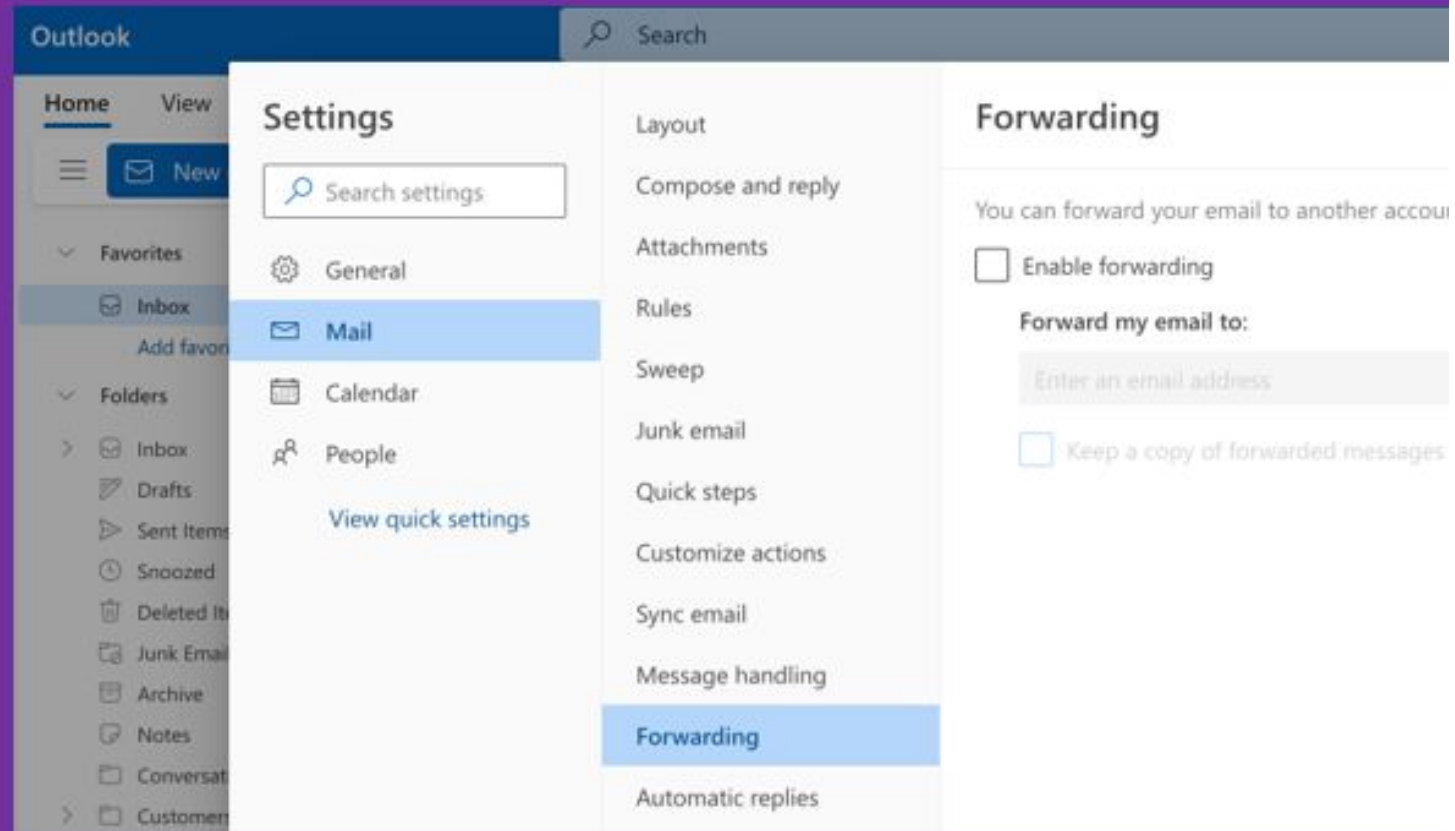
School of Communication 2240 Campus Drive

DISABLE EMAIL FORWARDING

Attackers 'forward' your email to themselves so they get a copy and can keep tabs on you

With Microsoft you have to check in Outlook Web > Settings > Mail

Forwarding should be globally disabled (or at least should trigger security alerts).



uBLOCK ORIGIN EXTENSION

Blocks Ads, malicious downloads, bad scripts, tracking cookies, and tons more

<https://uBlockOrigin.com/>

chris@freshtech.it
(860) 768-9300 x200

FRESH
TECH

uBlock Origin - Free, open-source ad content blocker.

Easy on CPU and memory.



1.46.0 - released 40 days ago



0.1.22.12266, experimental - released 42 days ago



Github (gorhill/uBlock)

The screenshot shows the uBlock Origin extension interface overlaid on a Facebook page. On the left, a list of blocked content categories is visible, including 'all', 'images', '3rd-party', 'inline scripts', '1st-party scripts', '3rd-party scripts', '3rd-party frames', 'facebook.com', 'www.facebook.com', 'doubleclick.net', and 'fbcdn.net'. On the right, a power button icon is displayed above the text 'www.facebook.com'. Below this, there are icons for various settings and a summary of blocked content: 'Blocked on this page 7 (3%)', 'Domains connected 2 out of 3', and 'Blocked since install 561,026 (7%)'. At the bottom, there are icons for 'More' and 'Less'.

uBlock Origin is not just an "ad blocker", it's a wide-spectrum content blocker with CPU and memory efficiency as a primary feature.

Thank You

Banking services powered by M&T Bank, Member FDIC.

References to “Clients’ Funds Trust Account (IOLTA / IOLA)” or “Interest on Lawyers Trust Account” shall be interpreted to include “IOLA,” or “Interest on Lawyer Account,” and “IOTA,” or “Interest on Trust Account,” as applicable in a particular state.

Nota is a product/service offered by M&T Bank. Use of Nota does not ensure compliance with state rules and regulations applicable to Clients’ Funds Trust Accounts (IOLTA / IOLA) . The advertised product/services and their features and availability are subject to change without notice at any time. Use of the product/service is subject to and governed by certain terms, conditions, and agreements required by Nota. Attorneys whose offices and practices are in NY, NJ, MD, PA, DE, CT, VA, DC, NH, MA, ME, VT, FL, or WV are eligible for banking products/services through M&T Bank. The use of such M&T banking services is subject to certain terms, conditions, and agreements required by M&T.

© 2024 M&T Bank. All Rights Reserved.