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

FRESHTECH

Nota by M&T Bank

Tarter Krinsky & Drogin

- 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

FRESHTECH

Nota
by M&T Bank

Tarter Krinsky & Drogin

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

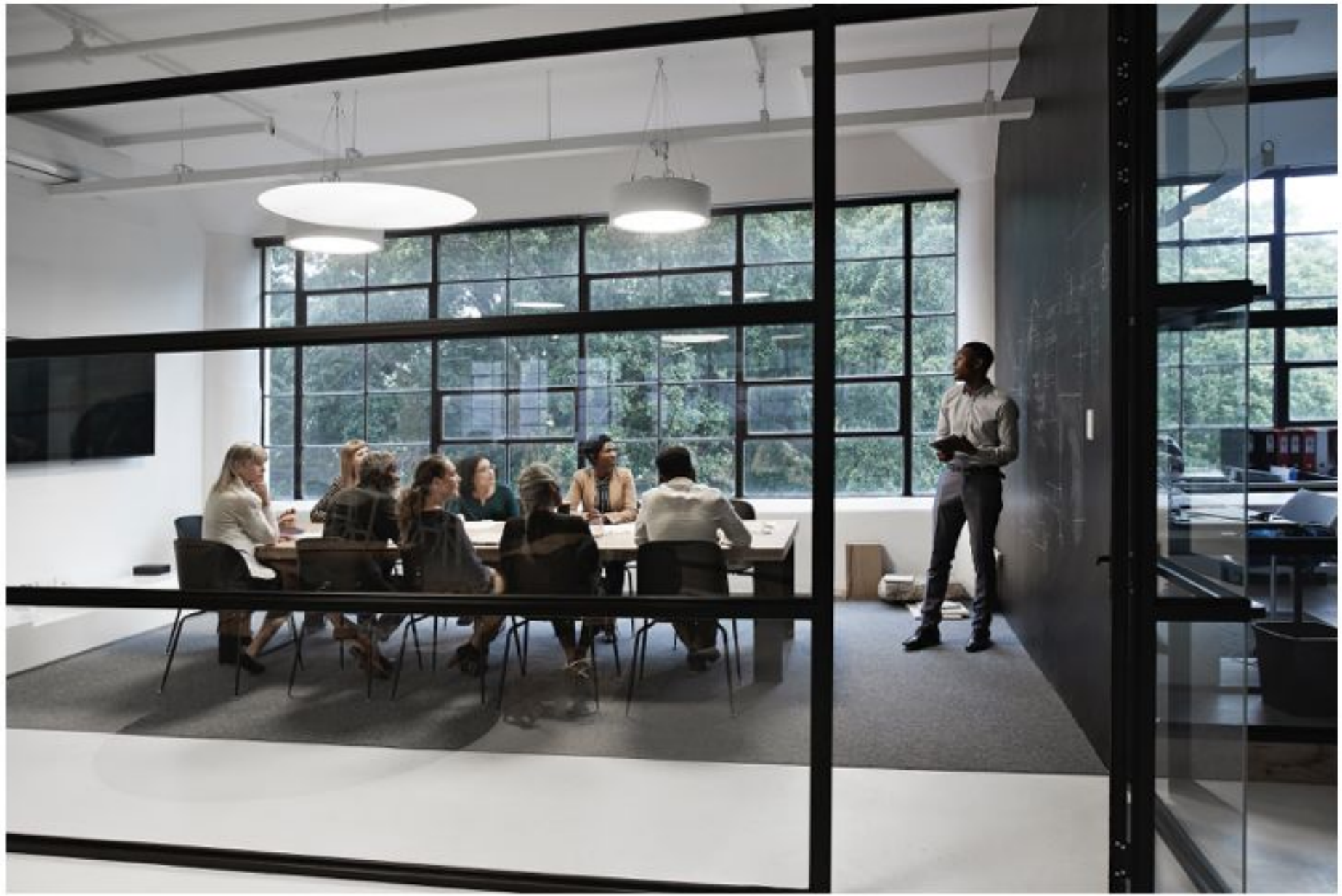
Unfortunately, even law firms are at risk for embezzlement at the hands of dishonest employees.

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
by M&T Bank

Tarter Krinsky & Drogin



FRESHTECH

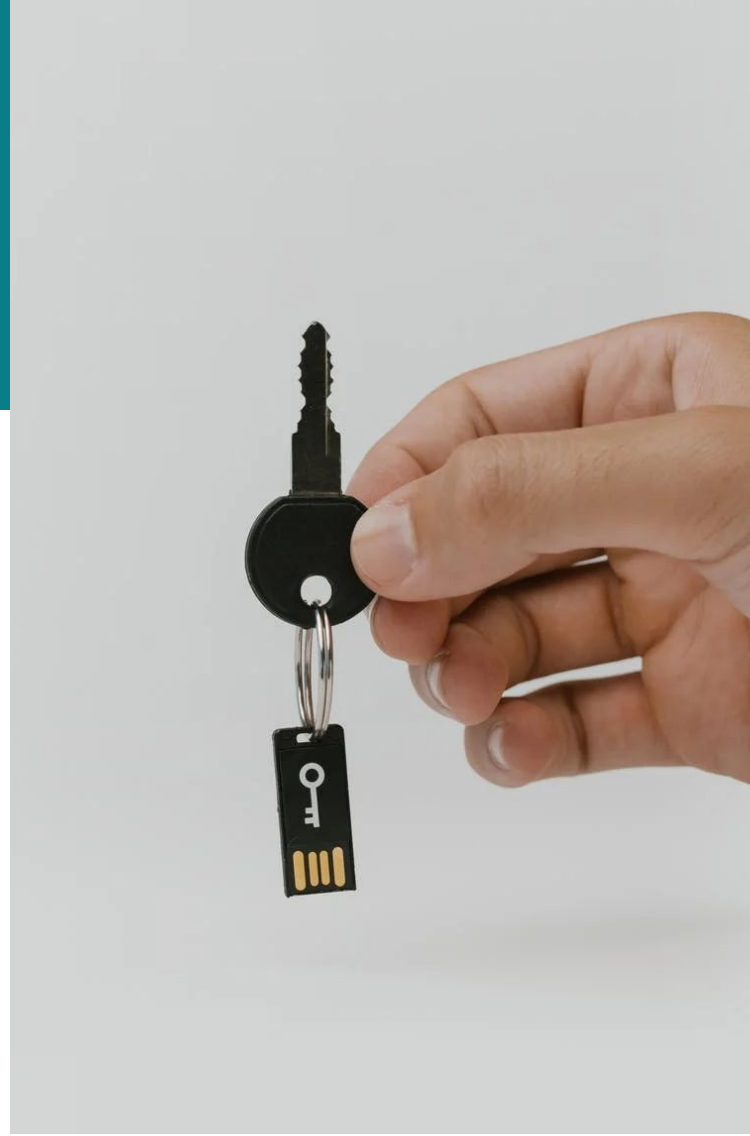
Nota
by M&T Bank

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

Consider Credit Cards/ACH

Get a Counterfeit Money Pen!

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:

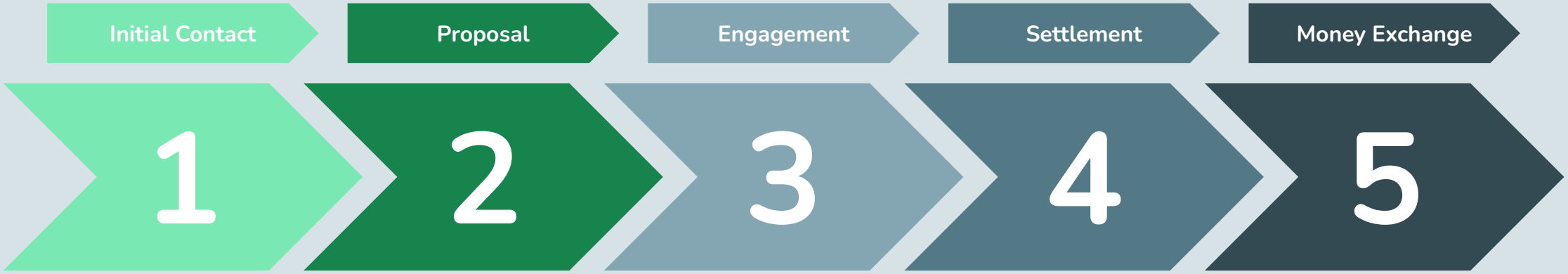
Ensure that the check was issued by a reputable bank

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.

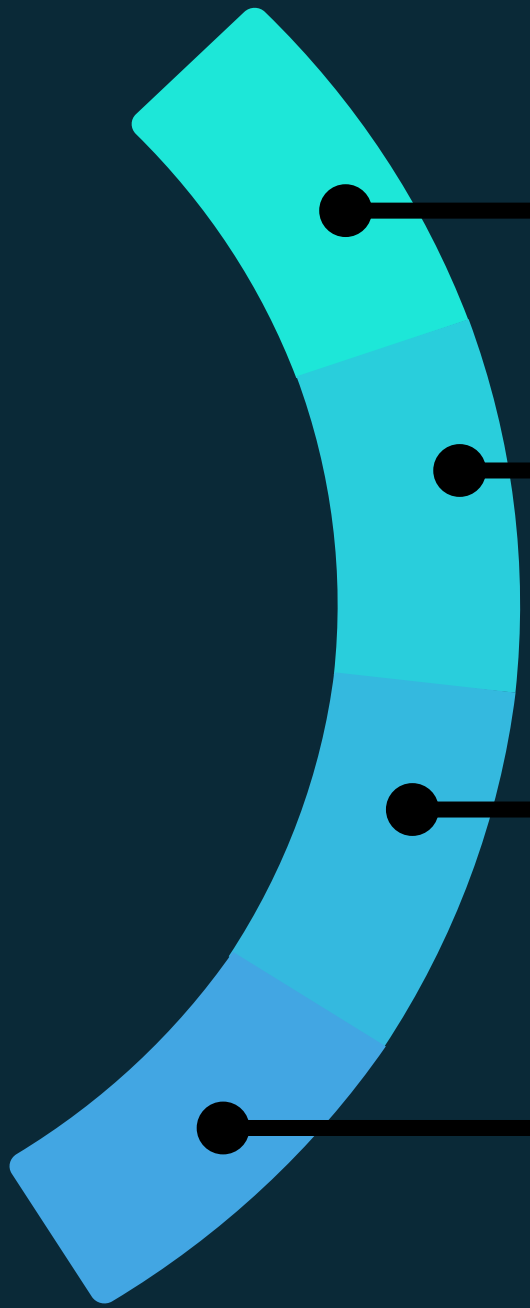
Attorney sends engagement letter, the scammer swiftly executes it.

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 acc

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.

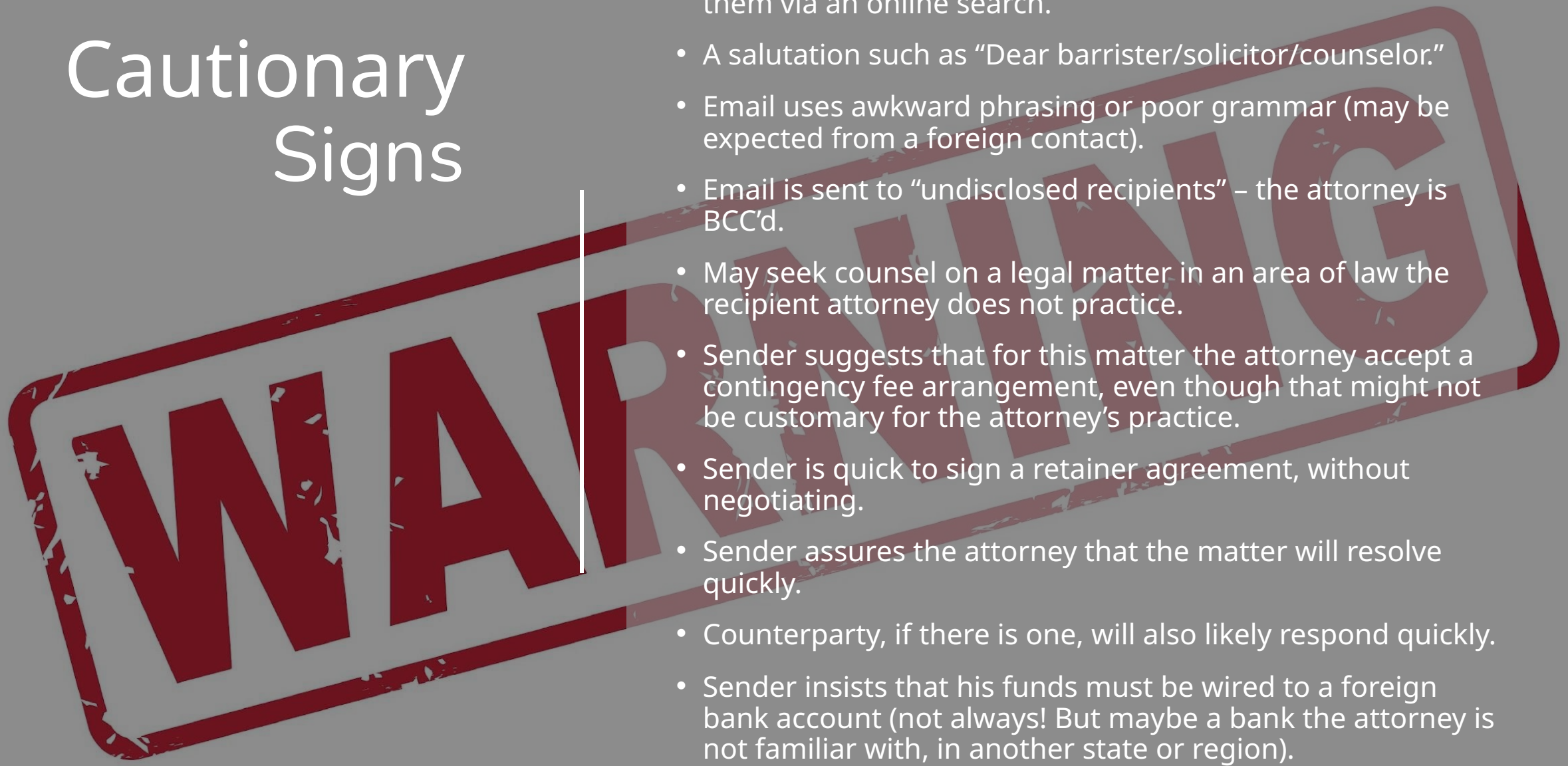
Take Your Time and Over-Communicate

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

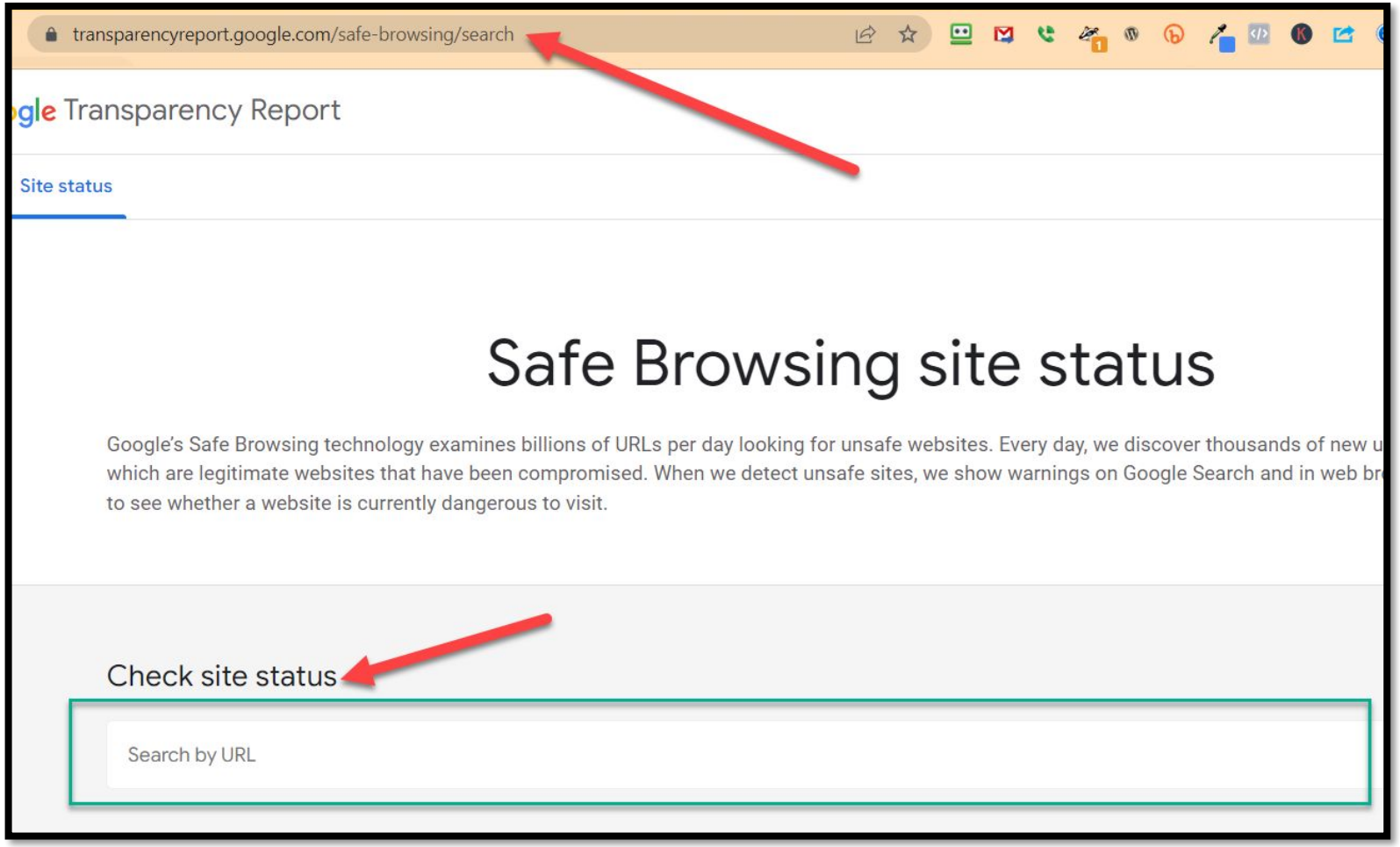


- Sender does not provide a referral source; says they found them via an online search.
- A salutation such as “Dear barrister/solicitor/counselor.”
- Email uses awkward phrasing or poor grammar (may be expected from a foreign contact).
- Email is sent to “undisclosed recipients” – the attorney is BCC’d.
- 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).

Nota
by M&T Bank

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 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

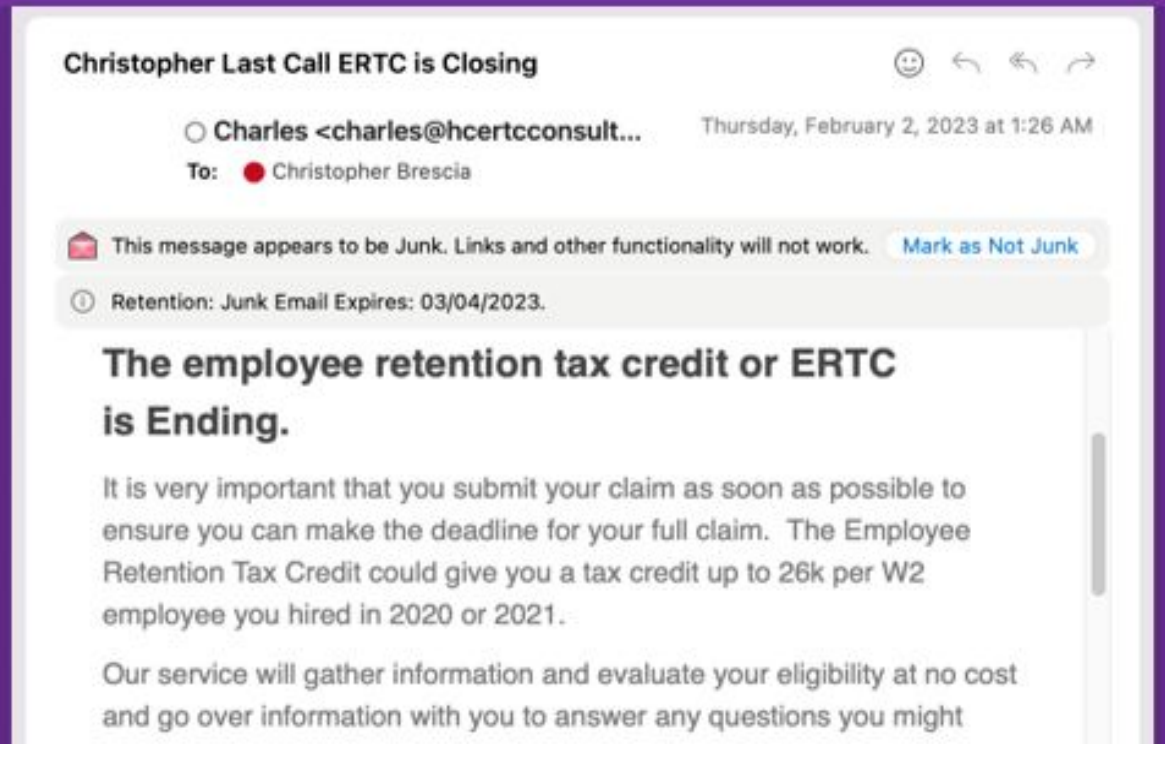
What they are

How they work

How you can defend against them

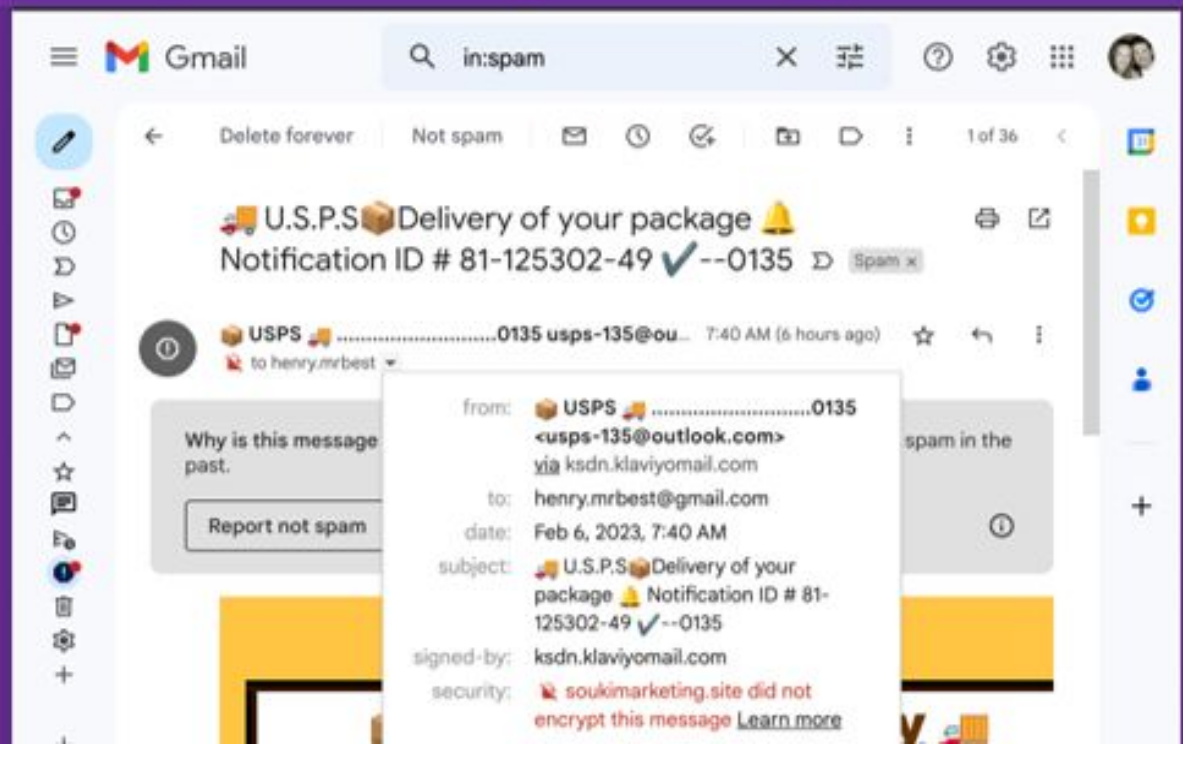
SPAM

Not lying, just not wanted.



PHISHING

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



PHISHING

Lying, with intent.

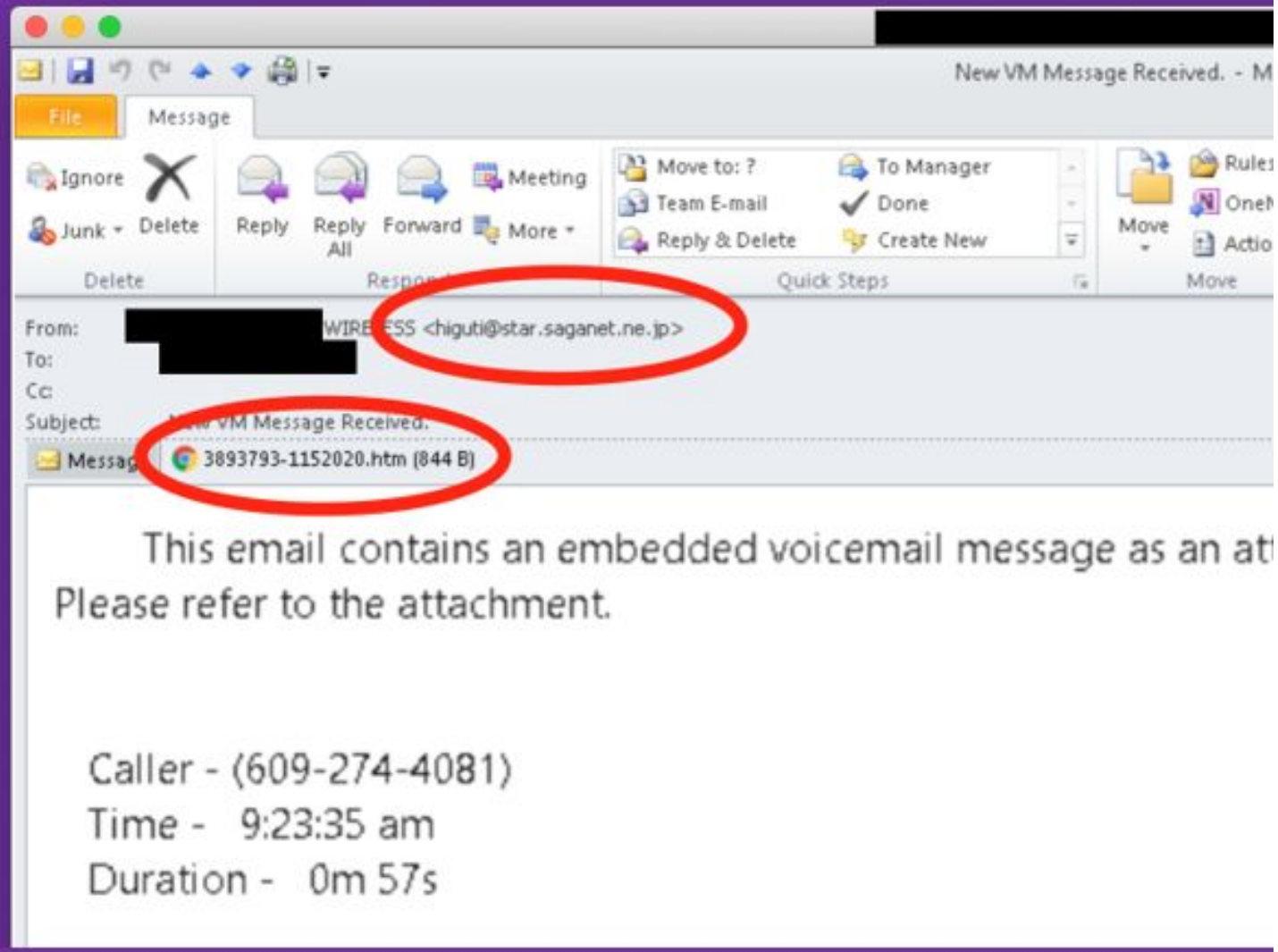
10:04 Phishing Email sent to CEO

11:36 CEO clicks Email

11:37 Attack launches

11:38 Finance gets Bogus Invoice

16:32 CEO realizes no emails in a while



PHISHING

Lying, with intent.

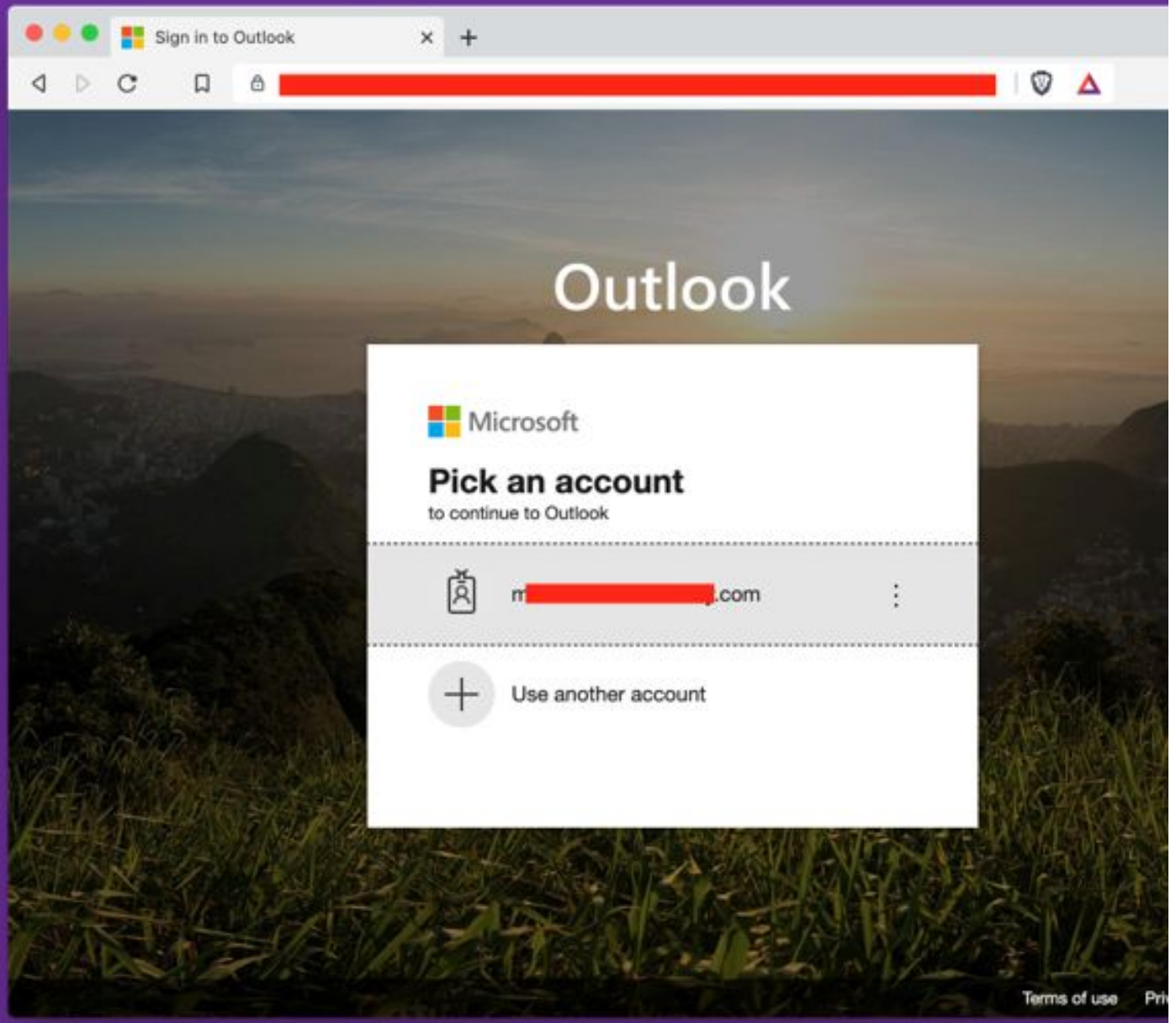
10:04 Malicious Email sent to CEO

11:36 CEO clicks Email

11:37 Attack launches

11:38 Finance gets Bogus Invoice

16:32 CEO realizes no emails in a while



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

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

[redacted]
----
Junk E-mail Rule
..
where my name [redacted] not in the To box
[redacted]ange.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.

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

Actual Nickname

Sent from CEOs real account

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

"urgency"

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

nonsense

[redacted] President
[redacted] (o)
(c)

Real signature

PHISHING

Lying, with intent.

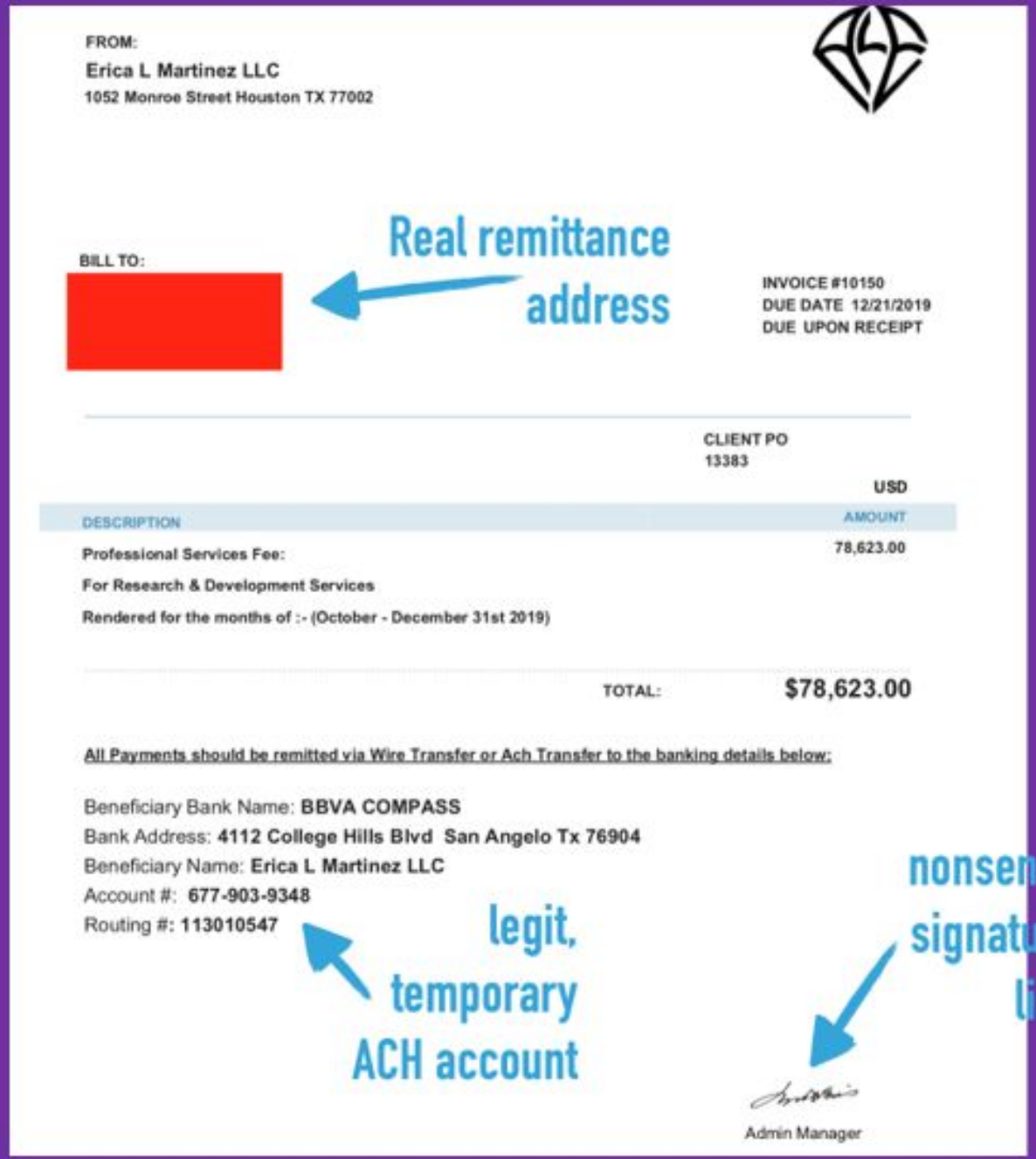
10:04 Malicious Email sent to CEO

11:36 CEO clicks Email

11:37 Attack launches

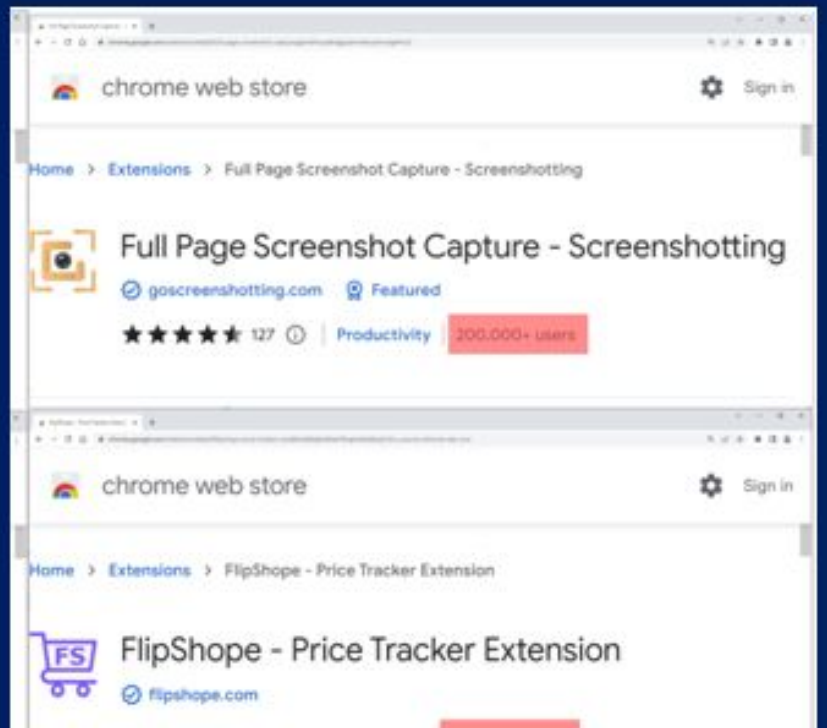
11:38 Finance gets Bogus Invoice

16:32 CEO realizes no emails in a while



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

↓

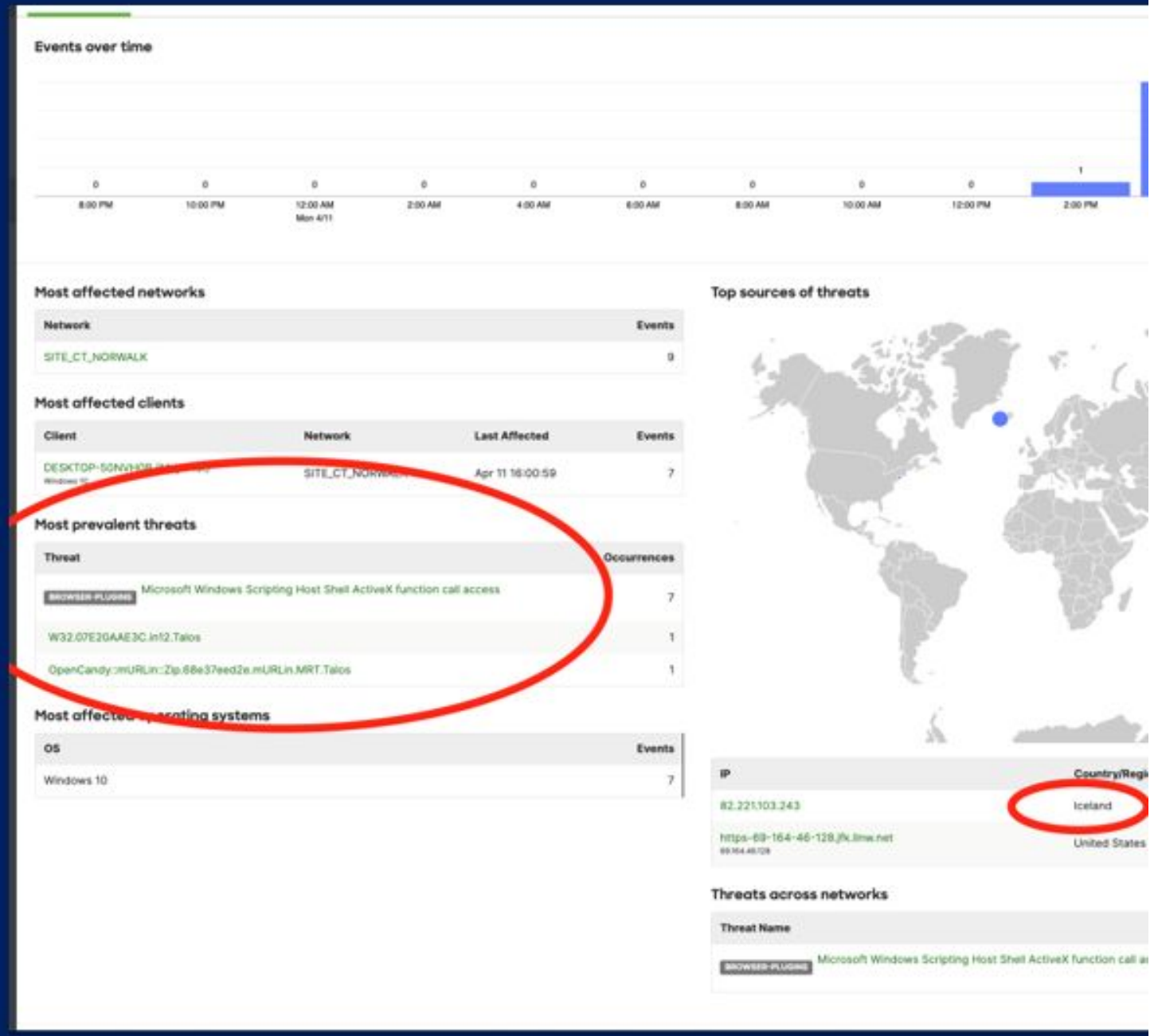
Trying to download more malware

↓

Payload from a driver download

↓

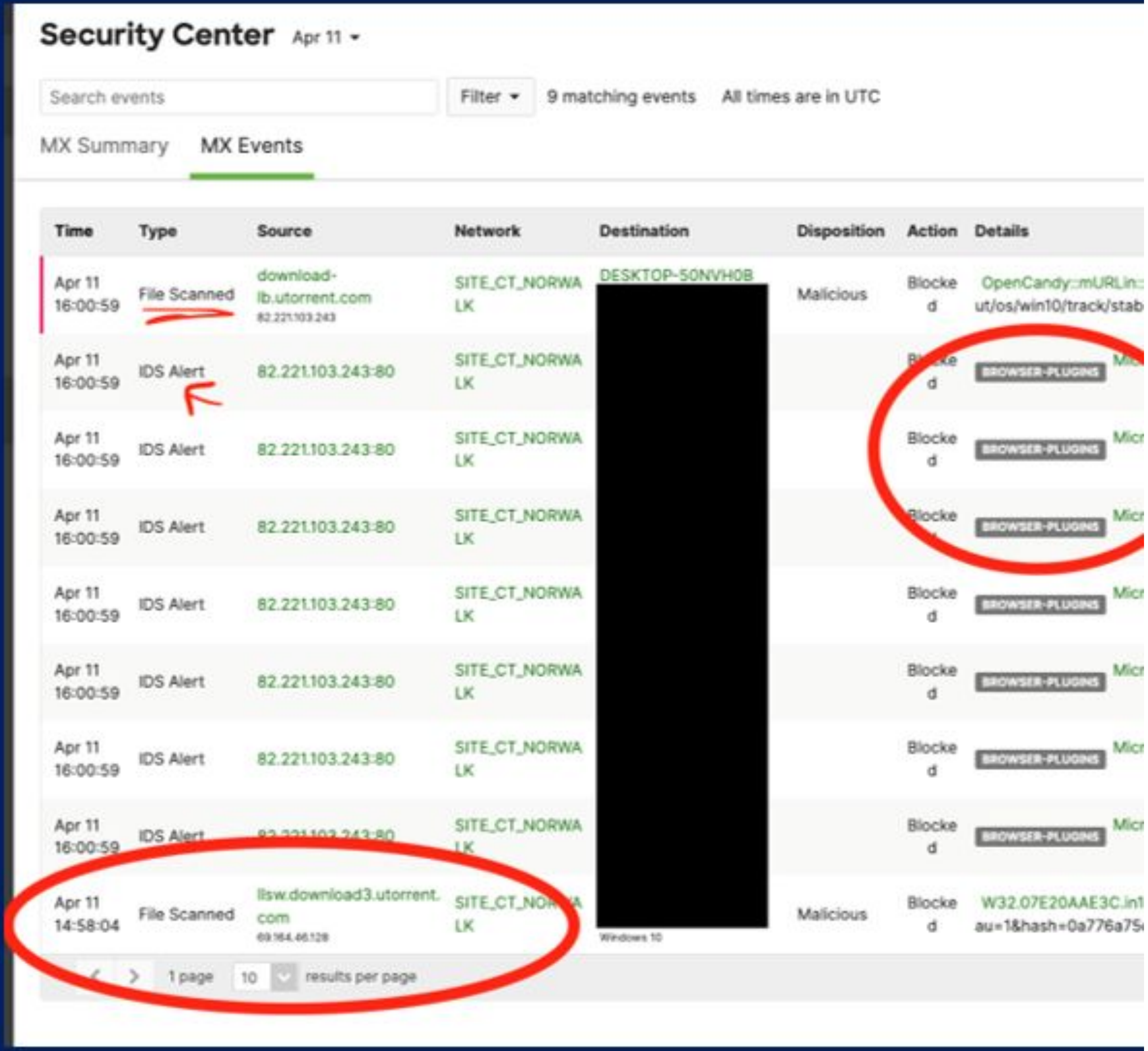
Payload included a Trojan



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

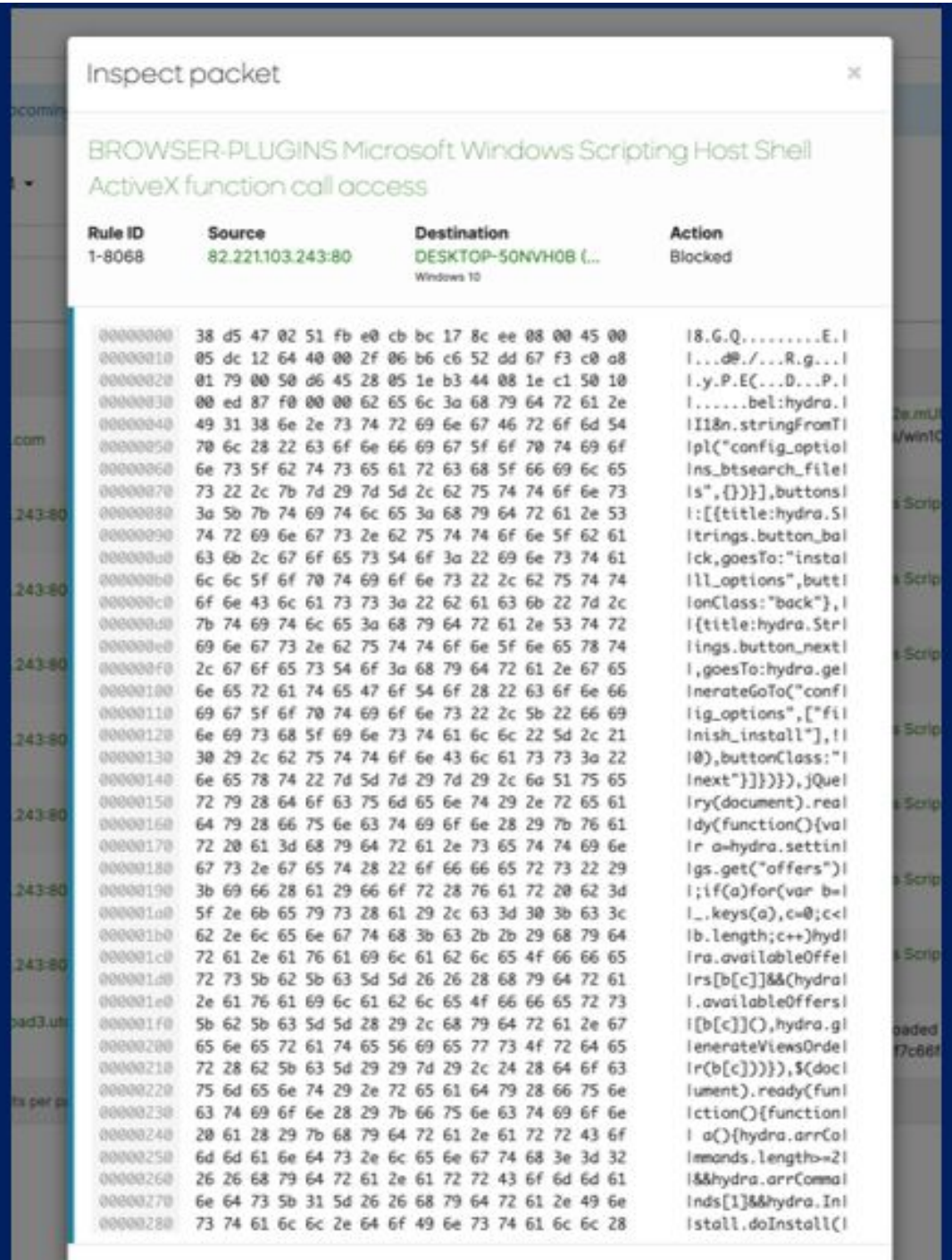
Time	Type	Source	Network	Destination	Disposition	Action	Details
Apr 11 16:00:59	File Scanned	download-lb.utorrent.com 82.221.103.243	SITE_CT_NORWALK	DESKTOP-50NVH0B [redacted]	Malicious	Blocked	OpenCandy::mURLin:: ut/os/win10/track/stab
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Mic
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Micr
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Micr
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Micr
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Micr
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Micr
Apr 11 16:00:59	IDS Alert	82.221.103.243:80	SITE_CT_NORWALK	[redacted]		Blocked	BROWSER-PLUGINS Micr
Apr 11 14:58:04	File Scanned	llsw.download3.utorrent.com 69.164.46.128	SITE_CT_NORWALK	[redacted] Windows 10	Malicious	Blocked	W32.07E20AAE3C.in1 au=1&hash=0a776a75

1 page | 10 | results per page

MALWARE

Bad programs, bad guys.

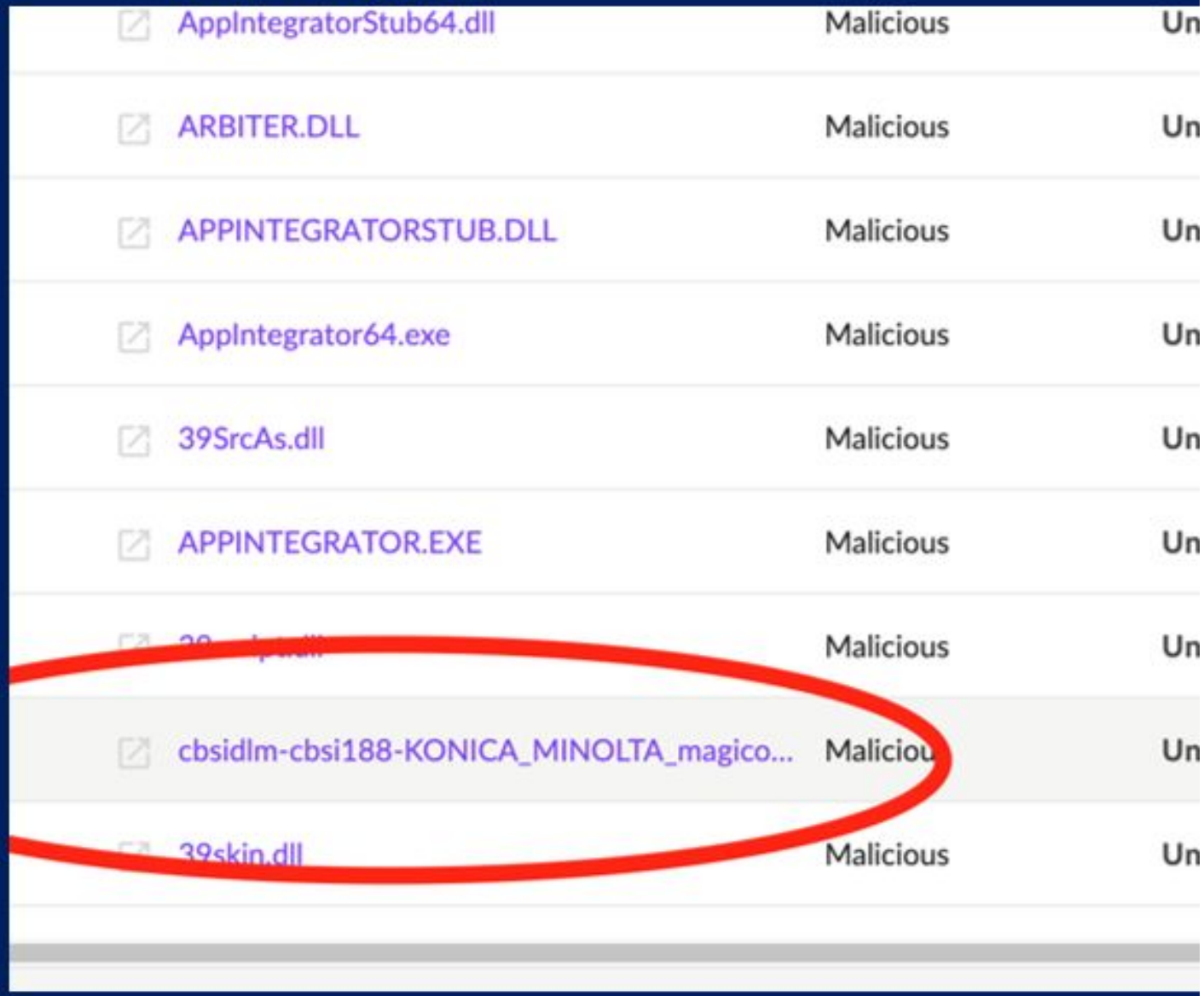
- Suspicious Traffic flagged on Firewall
- Coming from a Browser Extension
- Trying to download more malware
- Payload from a driver download
- Payload included a Trojan



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



MALWARE

Bad programs, bad guys.

Suspicious Traffic flagged on Firewall

↓

Coming from a Browser Extension

↓

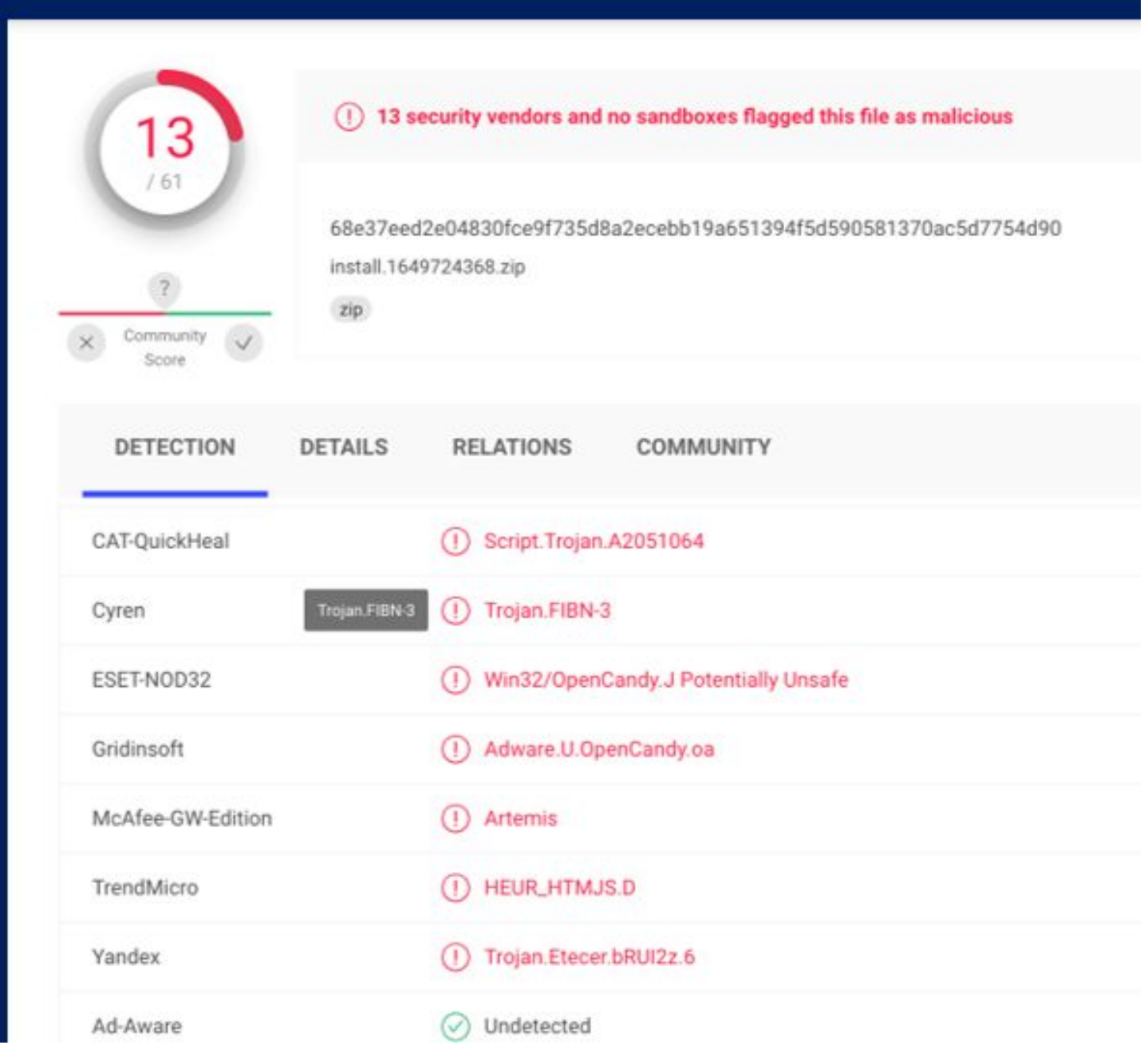
Trying to download more malware

↓

Payload from a driver download

↓

Payload included a Trojan



WIRE FRAUD

Tricking a victim into sending funds to an attackers account.

From: E[redacted]
Subject: New C[redacted] wire
Date: June 24, 2015 at 5:27 PM
To: Linda[redacted]

Hi Linda,

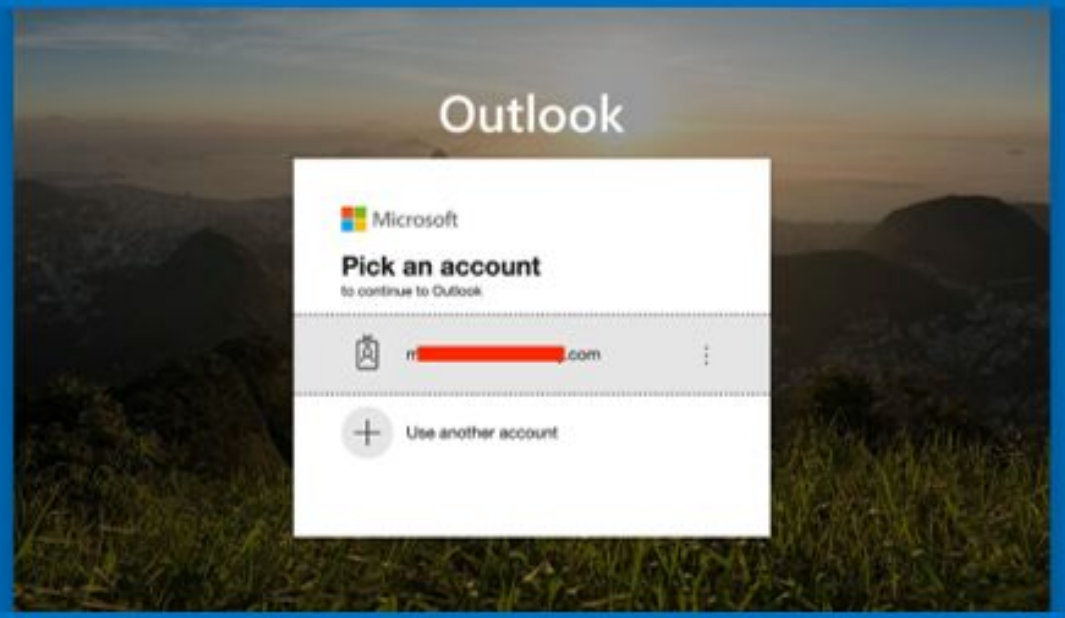
Please initiate a wire transfer for an amount of $50,000.
Execution should be no later than June 24, 2015.
The wire transfer information is:

Account # [redacted]
Routing number: 322271627 (Domestic Wires)
Swift Code --- CHASUS33 (for International wires)
Bank address: 10 S El Camino Real, Millbrae Ca 94030

The memo should say: "Funding Note Extension #3"

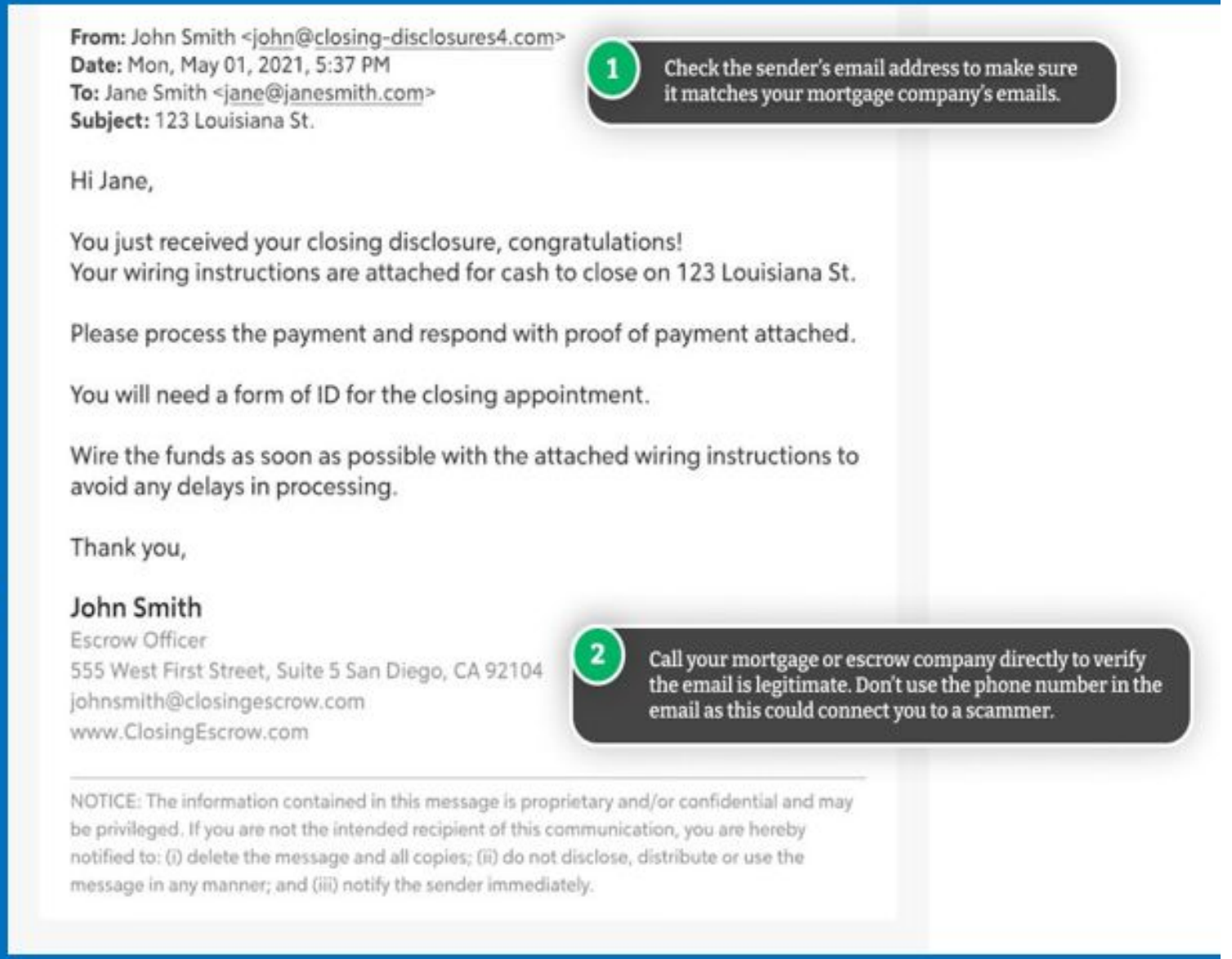
CRED. THEFT

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

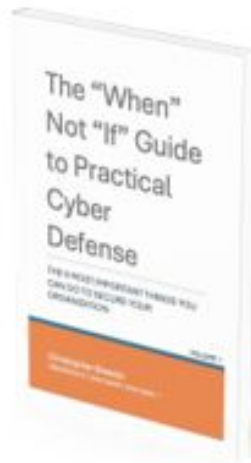
How you can defend against them

HOW TO DEFEND

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

FRESH TECH

- 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.

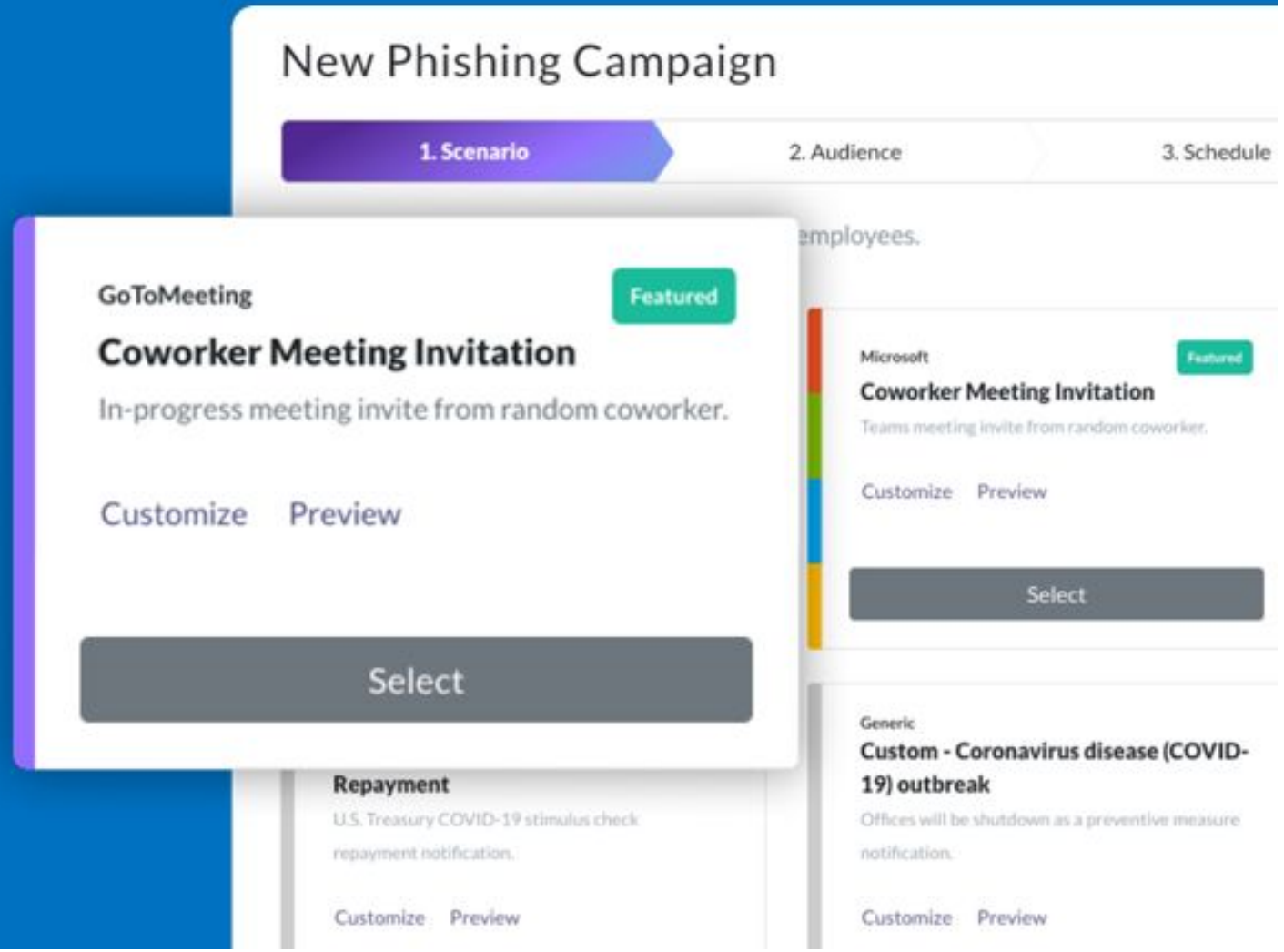
chris@freshtech.it
(860) 768-9300 x200

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

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

FRESH TECH

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 (866) 966-7226. 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: alttle.com and Bay National

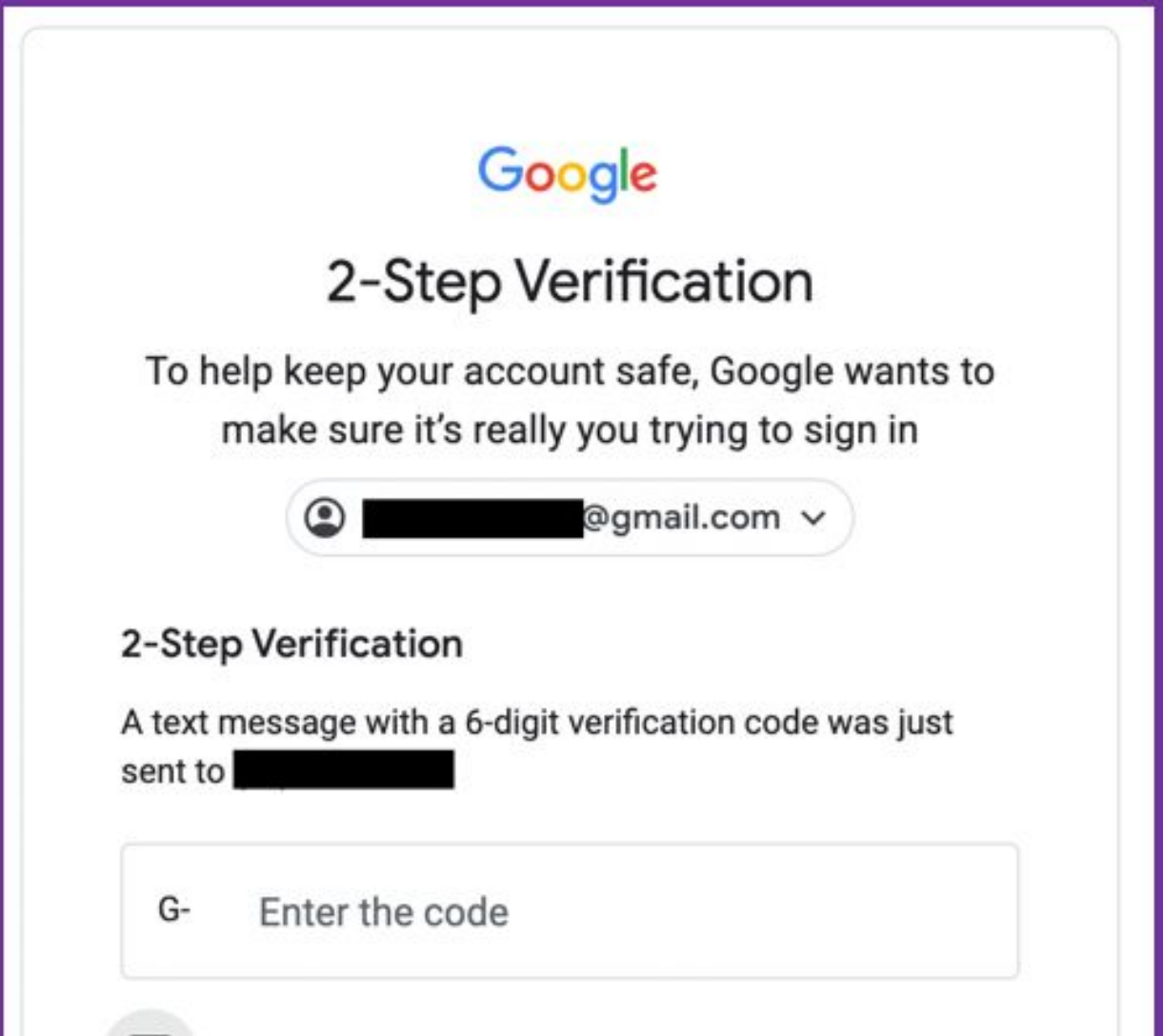
USE MULTI-FACTOR CODES

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

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

FRESH TECH

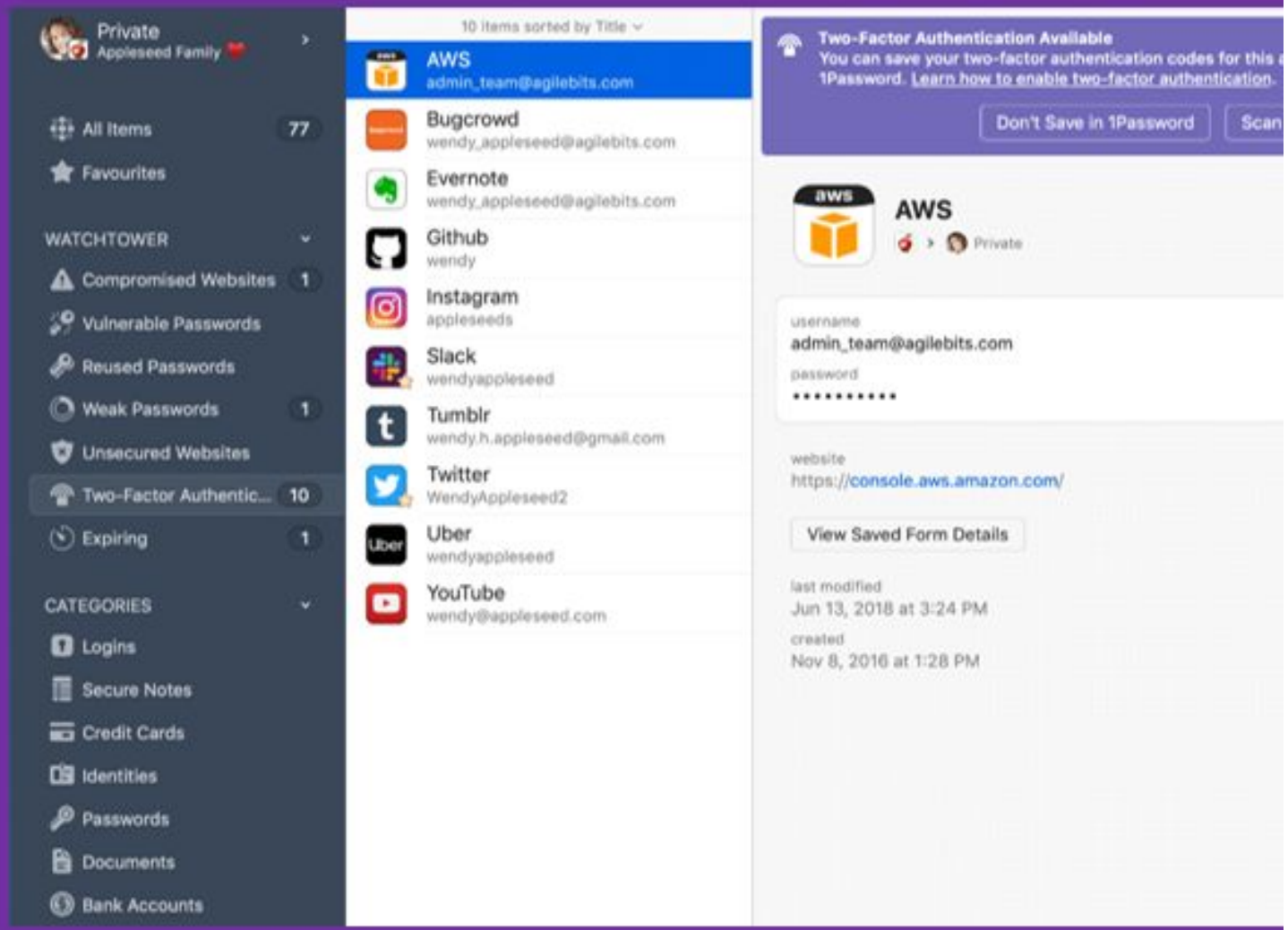
	Cyber Insurance Policy Coverage Comparison		
USER TIER	$250,000 Policy	$500,000 Policy	$1,000,000 Policy
LIMIT	$250,000	$500,000	$1,000,000
RETENTION/DEDUCTIBLE	NONE	$2,500	$2,500
ENTERPRISE SECURITY EVENT CLAIM	$250,000	$500,000	$1,000,000
PRIVACY REGULATION CLAIM	$250,000	$500,000	$1,000,000
CRISIS 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 INTERUPTION 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

FRESH TECH

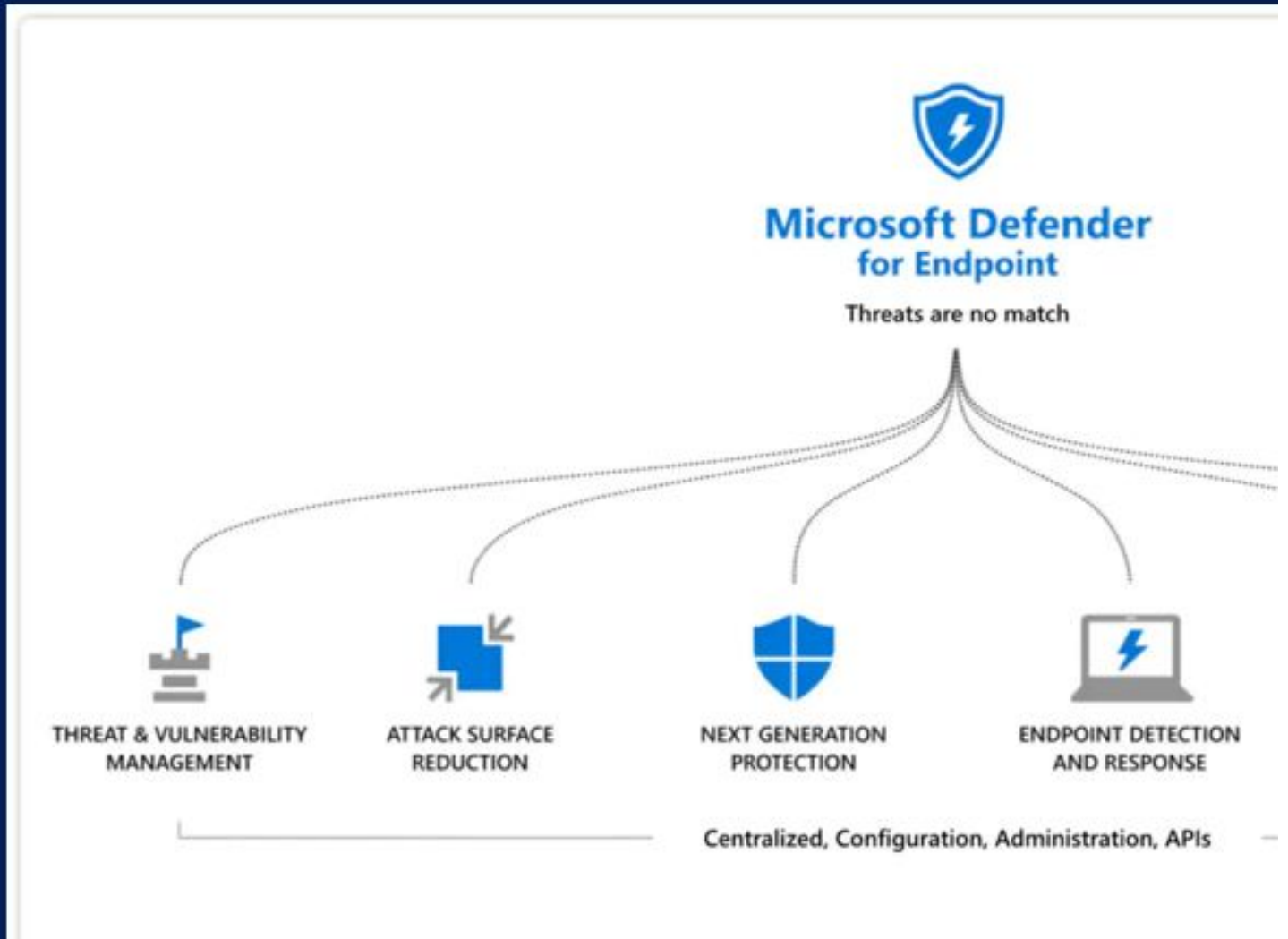
GET WINDOWS DEFENDER

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

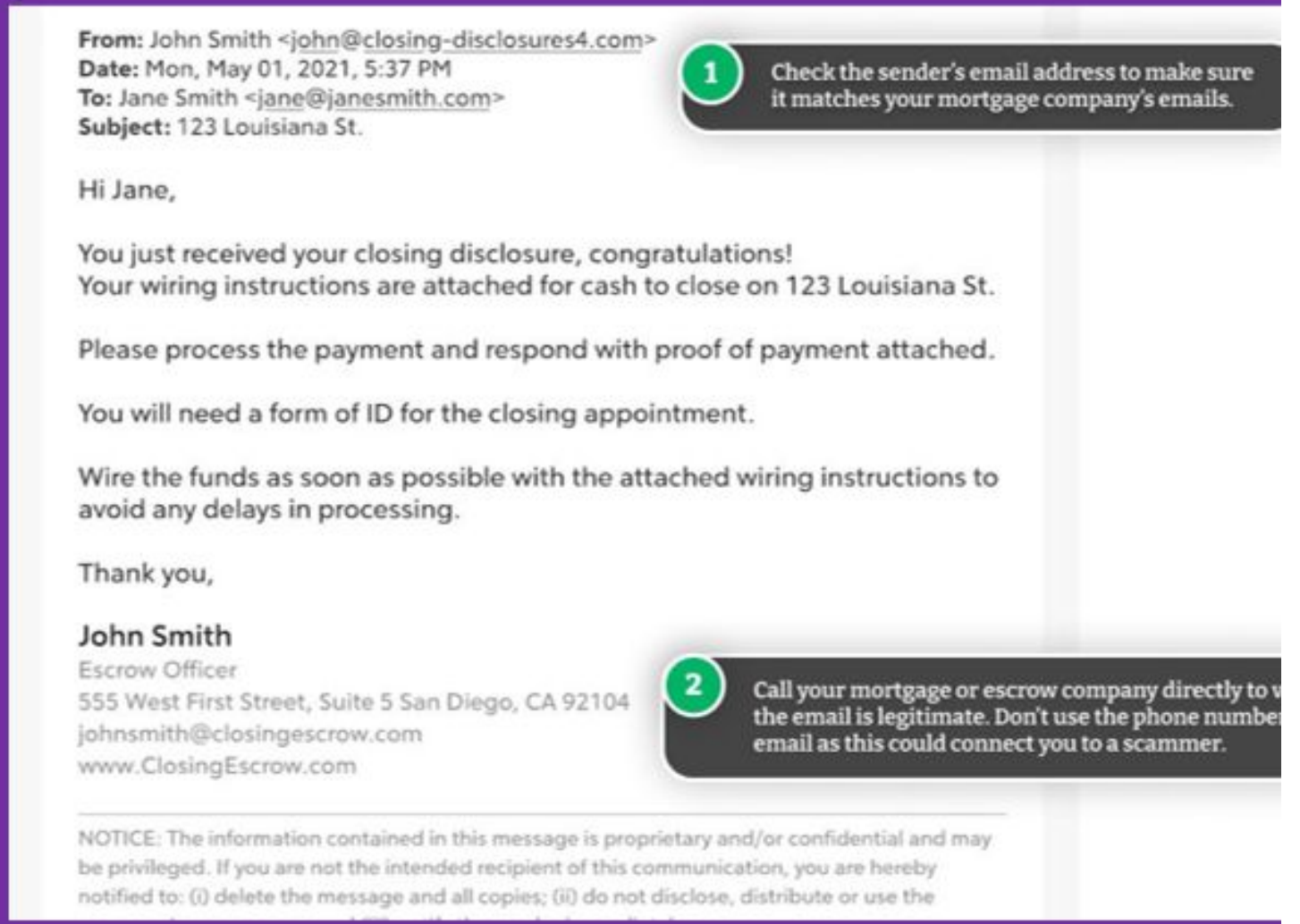
Don't call numbers, Don't reply to emails, Don't use unsubscribe links, Don't click attachments or do anything else with suspicious emails.

Get info directly from known sources.

Bad emails can look legit!

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

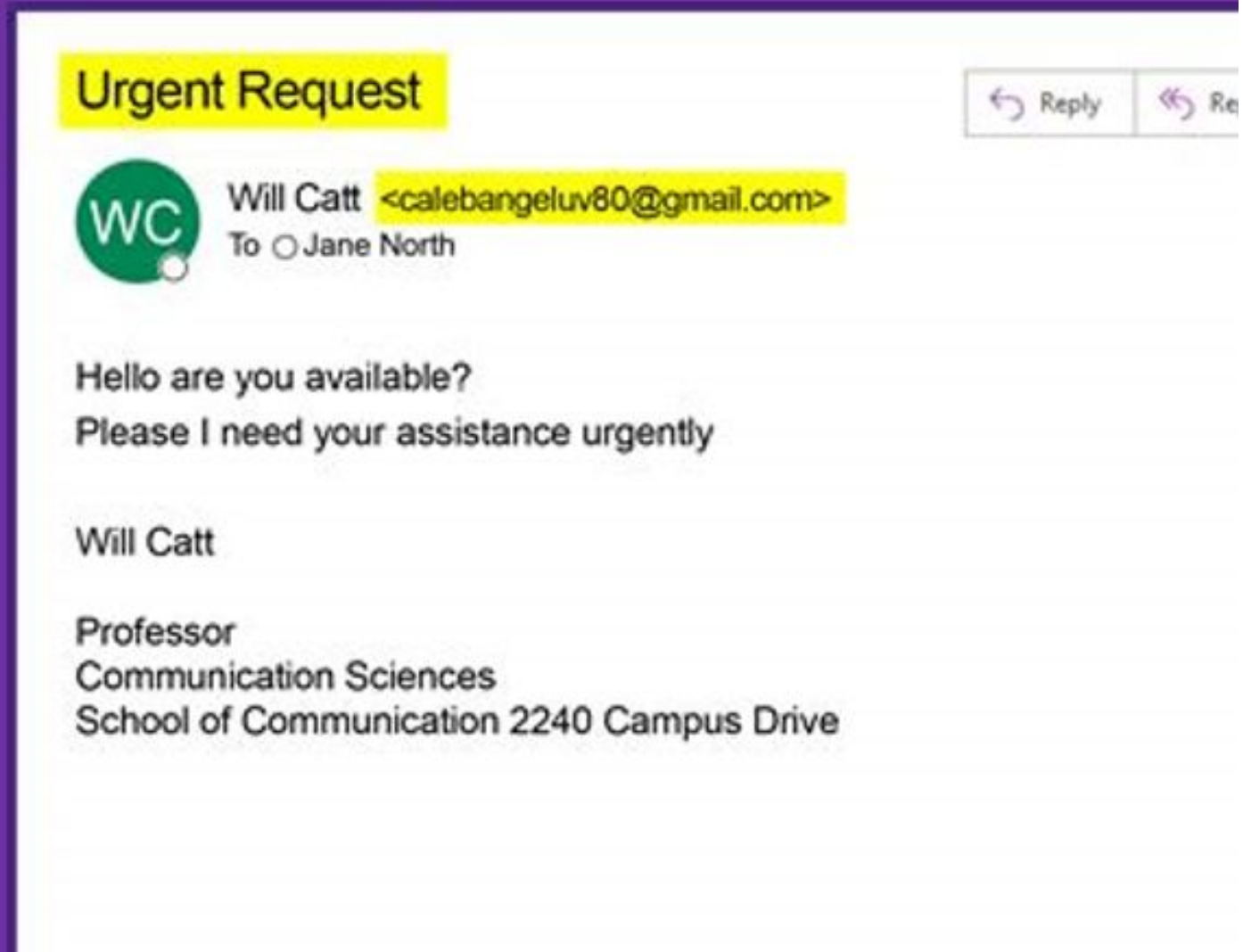
FRESH TECH



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

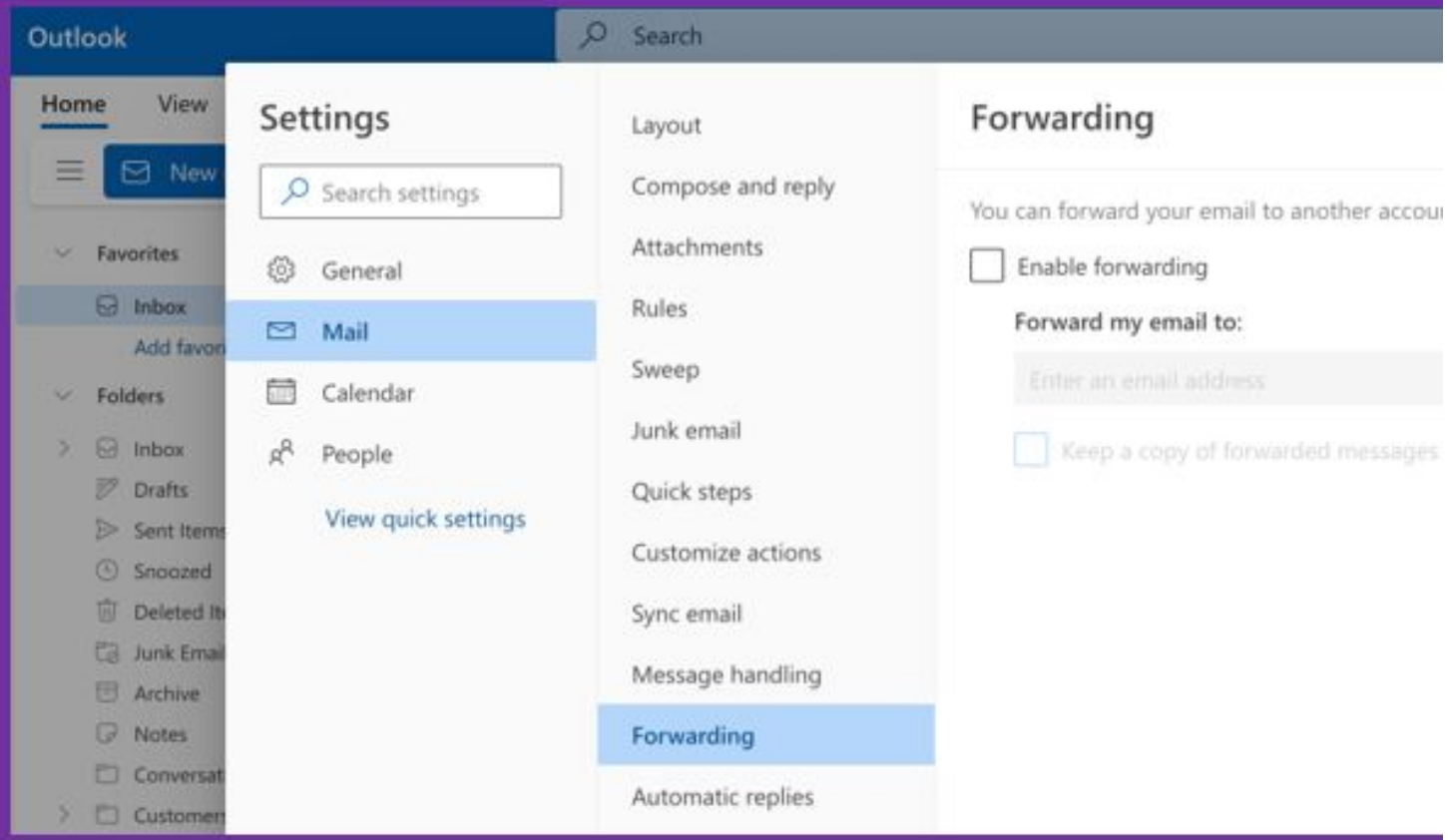
FRESH TECH

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

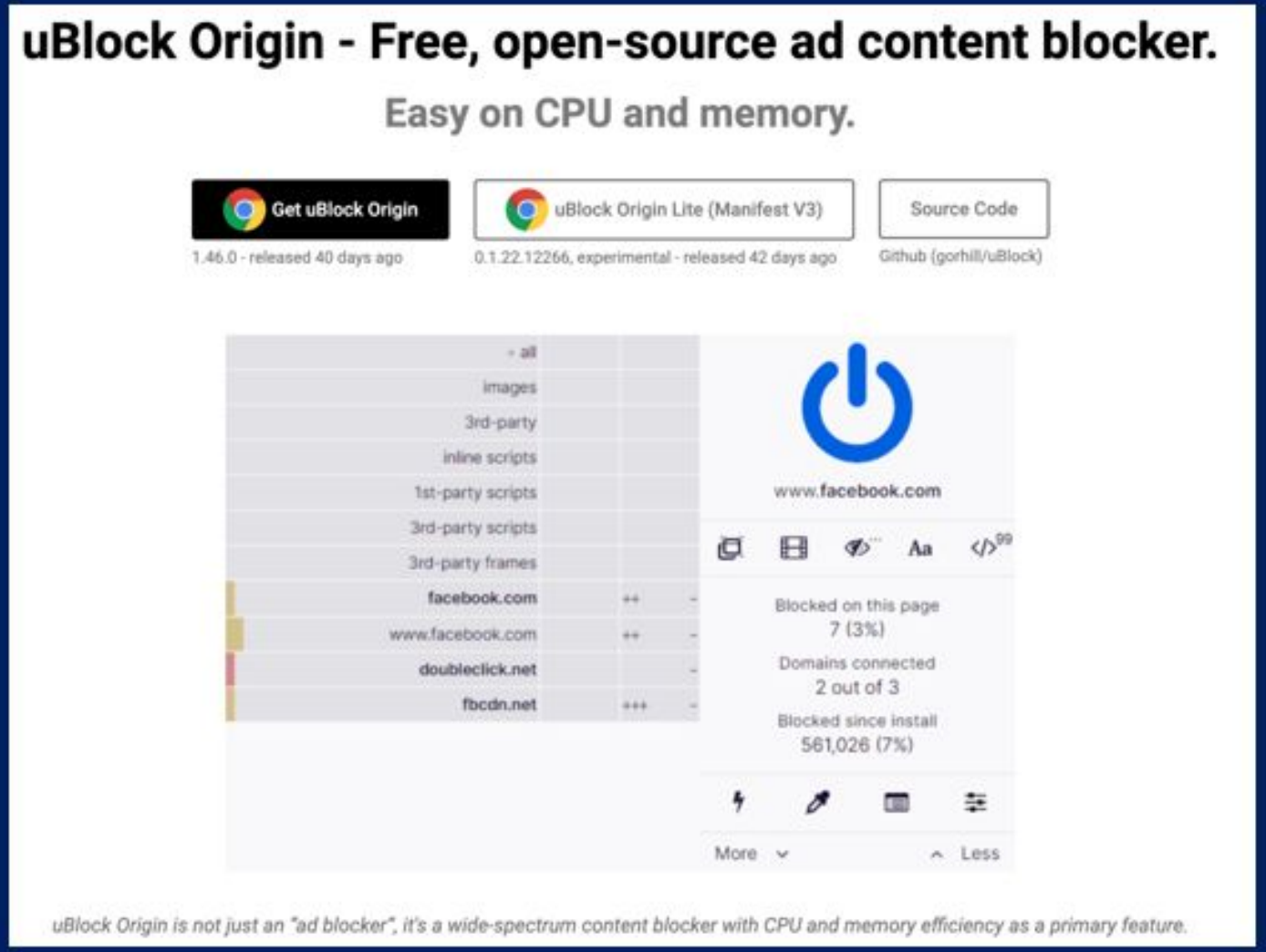
Forwarding should be globally disabled (or at least should trigger security alerts).



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

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.