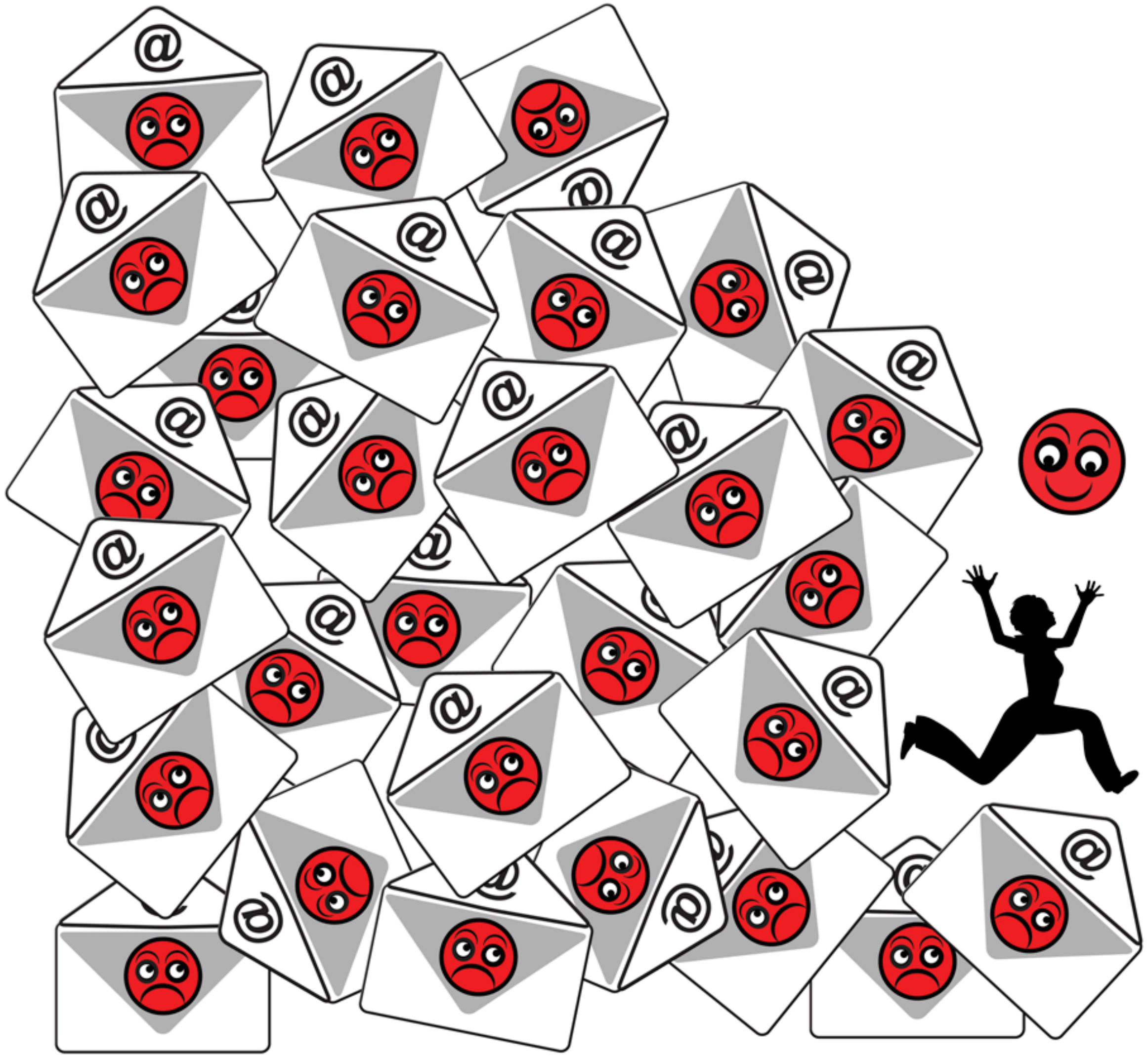
Recognize the Top Email Threats Hackers Use to Destroy Your Business

How to reduce the chances your business will be compromised via email scams.

ClearCom
IT Solutions

13 types of email threats being used by hackers today and the impact these email threats have on organizations.



ClearCom
IT Solutions

The 3-pronged approach ClearCom IT uses to minimize your organization's exposure to the havoc email threats can generate.

ClearCom
IT Solutions

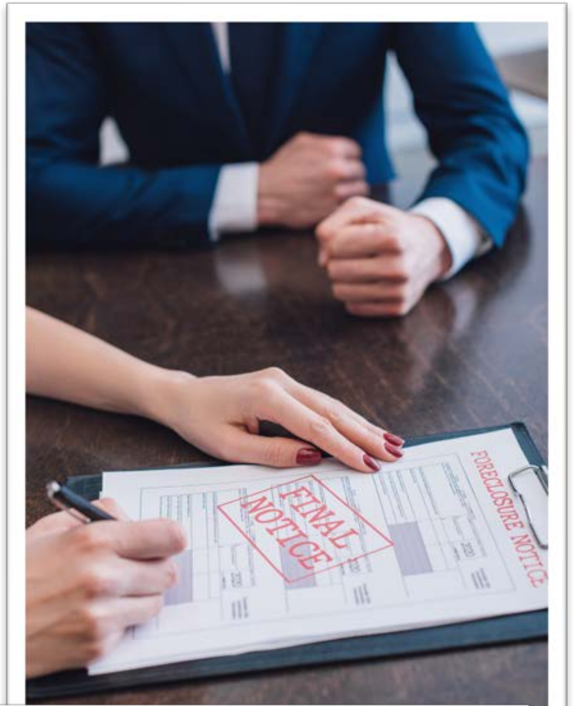
How to get your team trained to recognize these threats so they don’t accidentally fall victim to them.

ClearCom IT Solutions

Cybercrime cost $3.5 Billion in losses in 2019

Ransomware costs expected to reach $20 billion by 2021

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34



ClearCom
IT Solutions

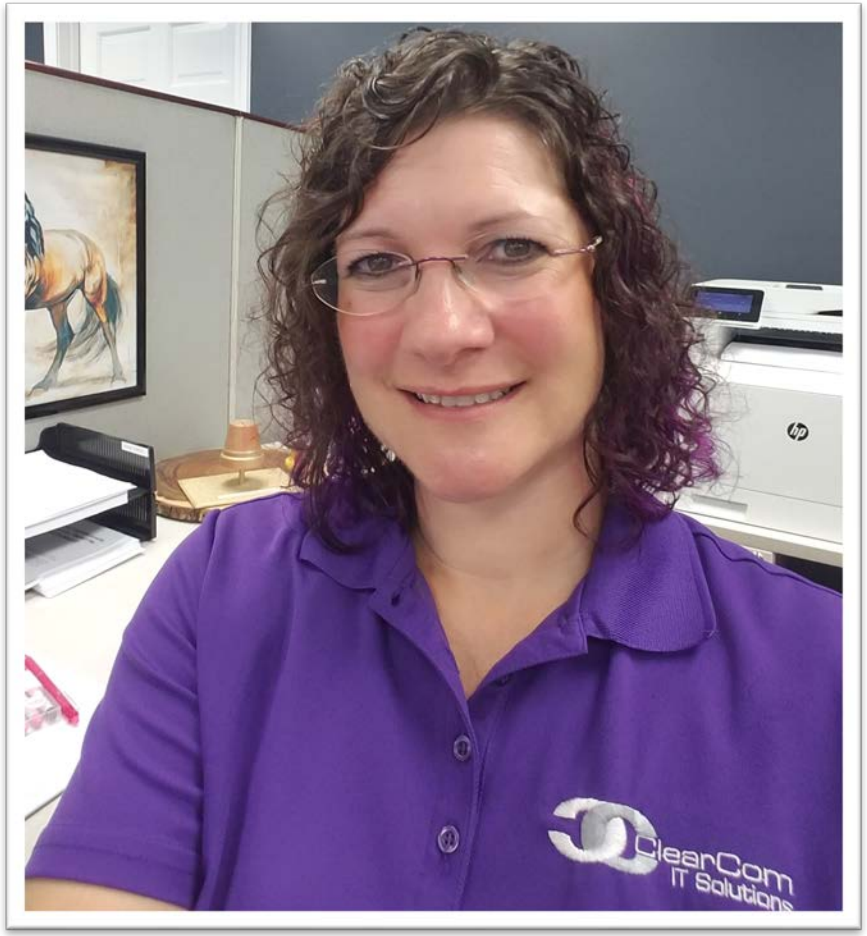
Wouldn't it be nice to not worry about clicking on a spam or phishing link that could compromise your data and/or network?

ClearCom
IT Solutions

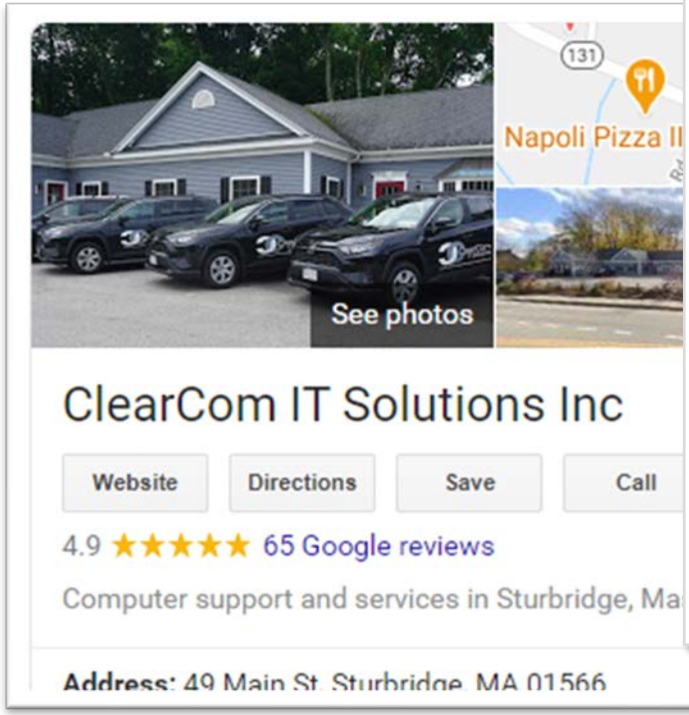
Jenn McGroary

Marketing & Administrative Coordinator

ClearCom IT Solutions, Inc.



ClearCom
IT Solutions



ClearCom IT Solutions Inc

4.9 ★★★★★ 65 Google reviews

Computer support and services in Sturbridge, Ma

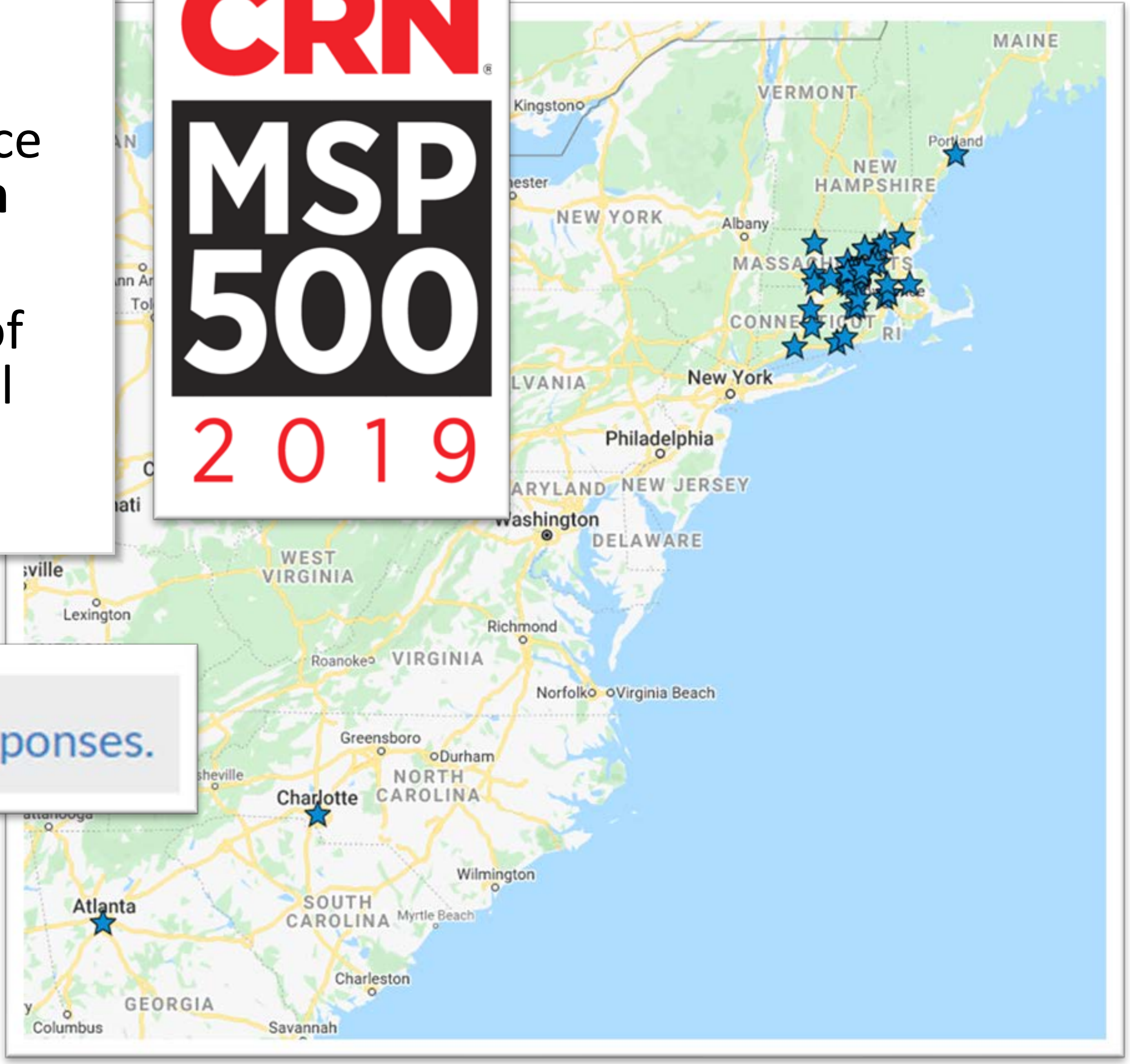
Address: 49 Main St, Sturbridge, MA 01566

- Named one of the top 10 IT companies in Central MA by Worcester Business Journal
- Selected as a Top 501 Global Managed Service Provider for the **fourth year in a row**
- 13 consecutive years of 100% contract renewal rate

2020 WINNER
MSP 501
Channel Futures

THE CHANNEL CO.
CRN
MSP 500
2019

★★★★★ (1,539) Unbiased customer responses.



ClearCom
IT Solutions

5 Categories of Email Threats

Spam

Malware

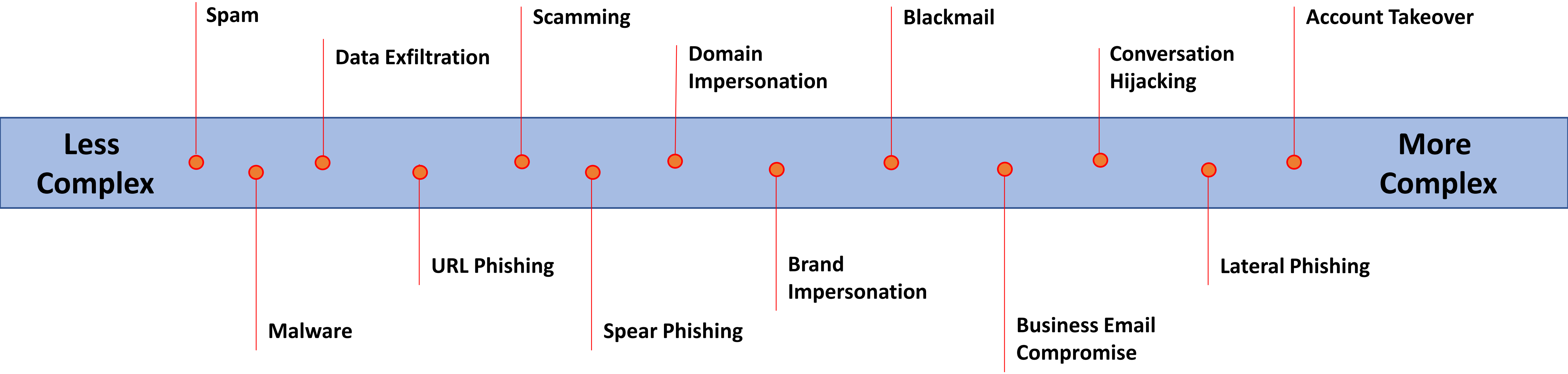
Data Exfiltration

Phishing Emails

Impersonation

ClearCom
IT Solutions

13 Different Types of Threats



Less Complex

Spam

Malware

Data Exfiltration

URL Phishing

Scamming

Spear Phishing

Domain Impersonation

Brand Impersonation

Blackmail

Business Email Compromise

Conversation Hijacking

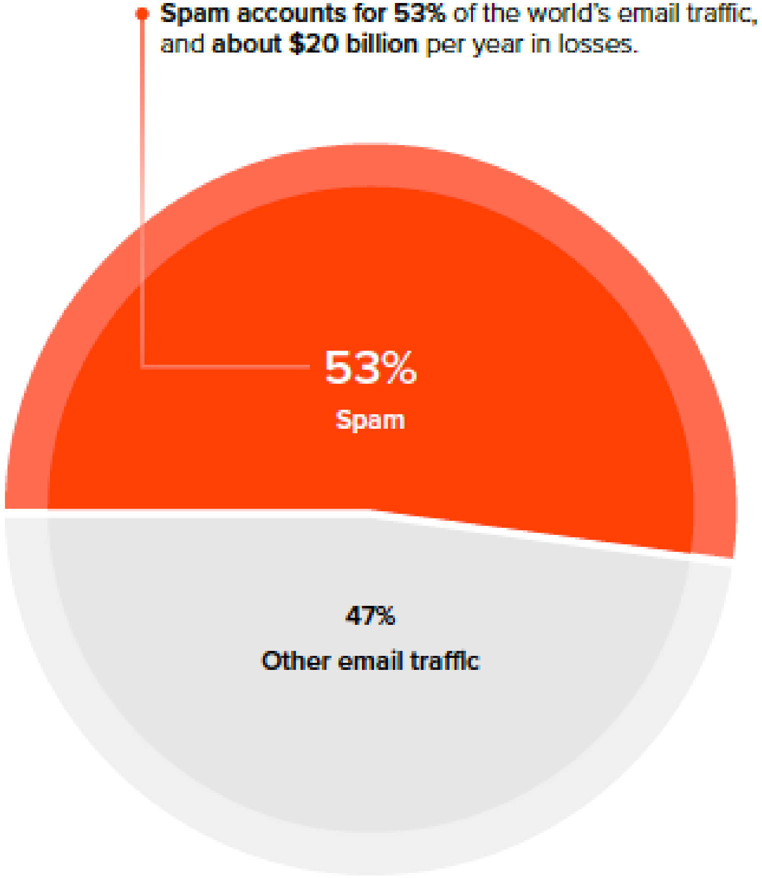
Lateral Phishing

Account Takeover

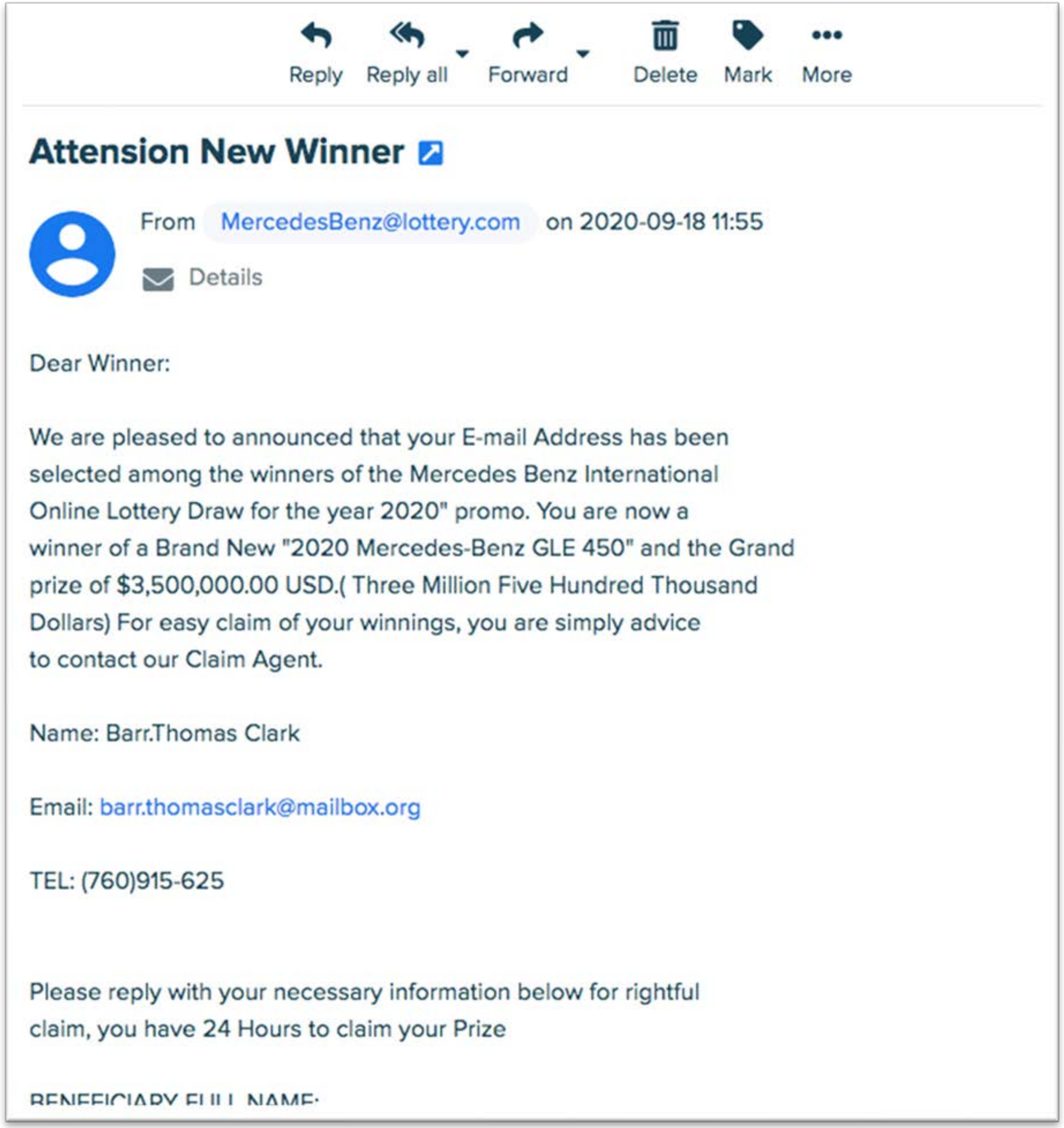
More Complex

ClearCom
IT Solutions

Spam



Spam accounts for 53% of the world's email traffic, and **about $20 billion** per year in losses.



Attension New Winner

From MercedesBenz@lottery.com on 2020-09-18 11:55

Dear Winner:

We are pleased to announced that your E-mail Address has been selected among the winners of the Mercedes Benz International Online Lottery Draw for the year 2020" promo. You are now a winner of a Brand New "2020 Mercedes-Benz GLE 450" and the Grand prize of $3,500,000.00 USD.(Three Million Five Hundred Thousand Dollars) For easy claim of your winnings, you are simply advice to contact our Claim Agent.

Name: Barr.Thomas Clark

Email: barr.thomasclark@mailbox.org

TEL: (760)915-625

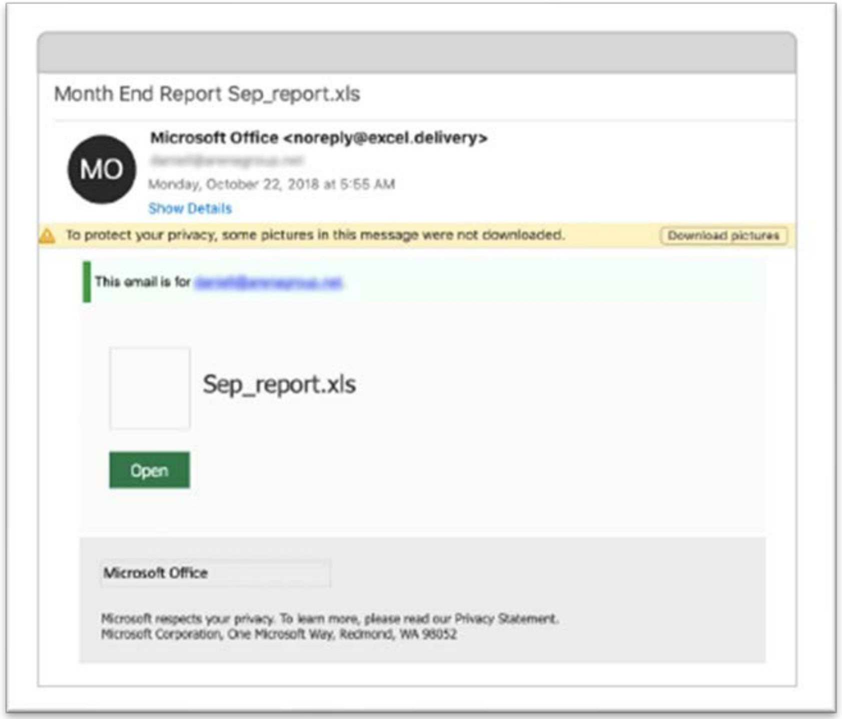
Please reply with your necessary information below for rightful claim, you have 24 Hours to claim your Prize

BENEFICIARY FULL NAME:

ClearCom
IT Solutions

Malware

94% of malware is delivered via email



Month End Report Sep_report.xls

Microsoft Office <noreply@excel.delivery>
[redacted]
Monday, October 22, 2018 at 5:55 AM
Show Details

⚠ To protect your privacy, some pictures in this message were not downloaded. Download pictures

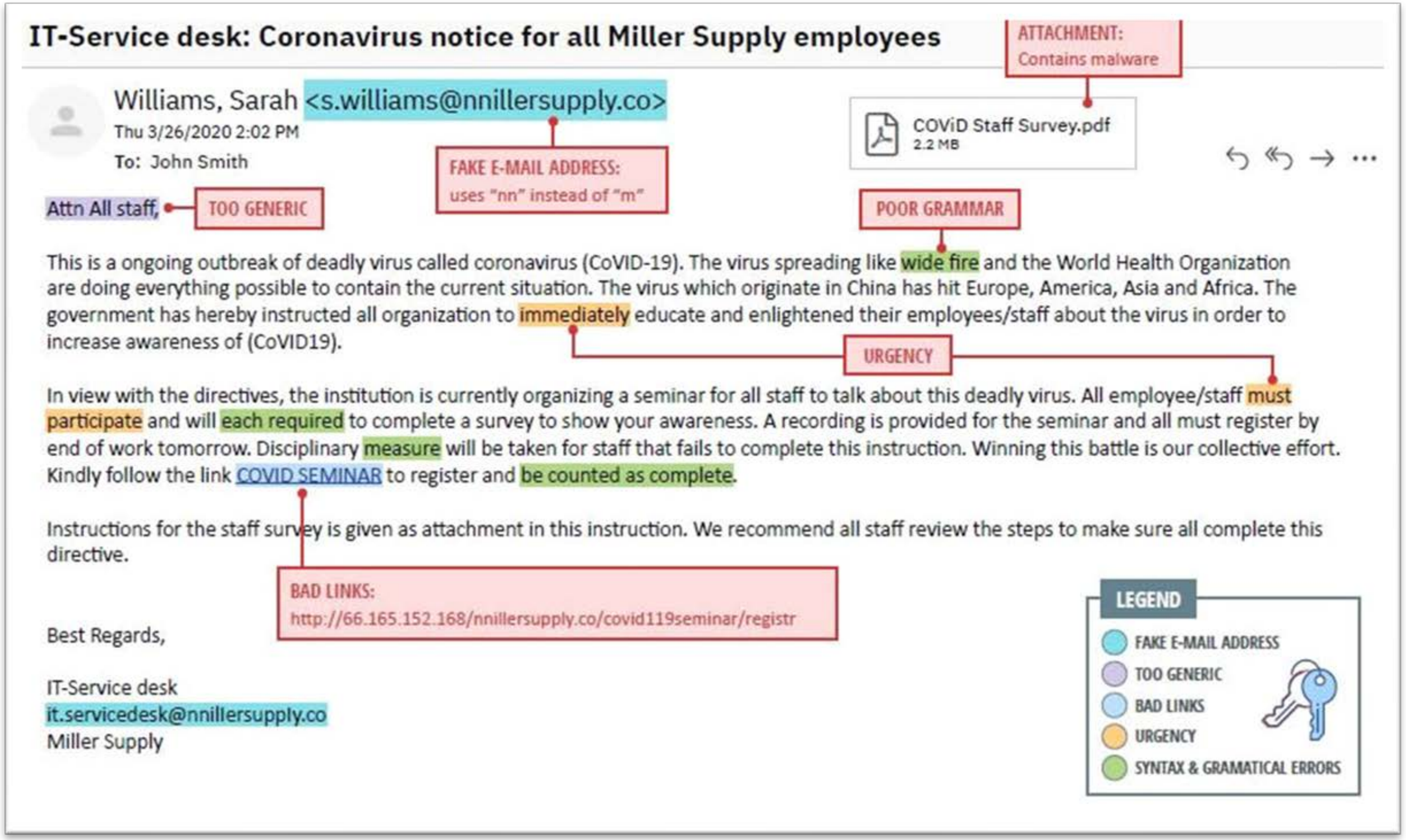
This email is for [redacted]

Sep_report.xls

Open

Microsoft Office

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



IT-Service desk: Coronavirus notice for all Miller Supply employees

ATTACHMENT:
Contains malware

Williams, Sarah <s.williams@nnillersupply.co>
Thu 3/26/2020 2:02 PM
To: John Smith

COViD Staff Survey.pdf
2.2 MB

FAKE E-MAIL ADDRESS:
uses "nn" instead of "m"

Attn All staff,

TOO GENERIC

POOR GRAMMAR

This is a ongoing outbreak of deadly virus called coronavirus (CoVID-19). The virus spreading like wide fire and the World Health Organization are doing everything possible to contain the current situation. The virus which originate in China has hit Europe, America, Asia and Africa. The government has hereby instructed all organization to immediately educate and enlightened their employees/staff about the virus in order to increase awareness of (CoVID19).

URGENCY

In view with the directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff must participate and will each required to complete a survey to show your awareness. A recording is provided for the seminar and all must register by end of work tomorrow. Disciplinary measure will be taken for staff that fails to complete this instruction. Winning this battle is our collective effort. Kindly follow the link COVID SEMINAR to register and be counted as complete.

Instructions for the staff survey is given as attachment in this instruction. We recommend all staff review the steps to make sure all complete this directive.

BAD LINKS:
http://66.165.152.168/nnillersupply.co/covid119seminar/registr

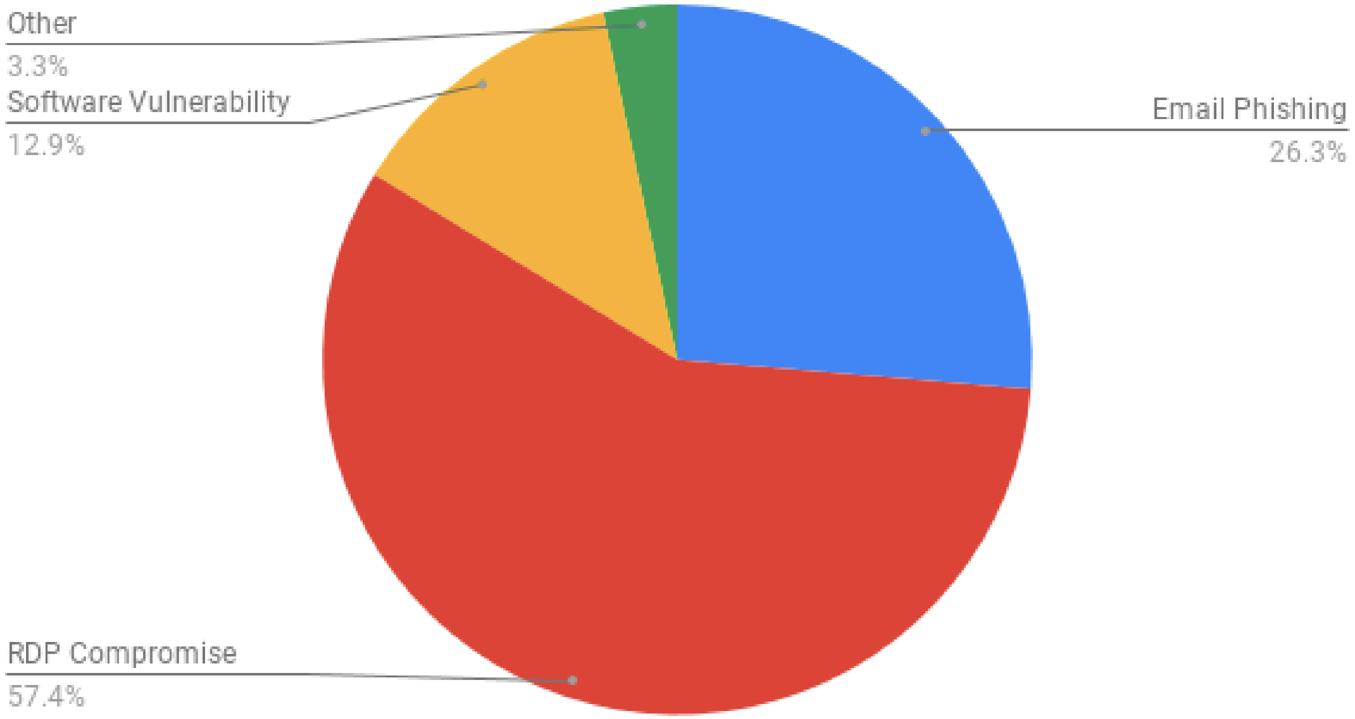
Best Regards,

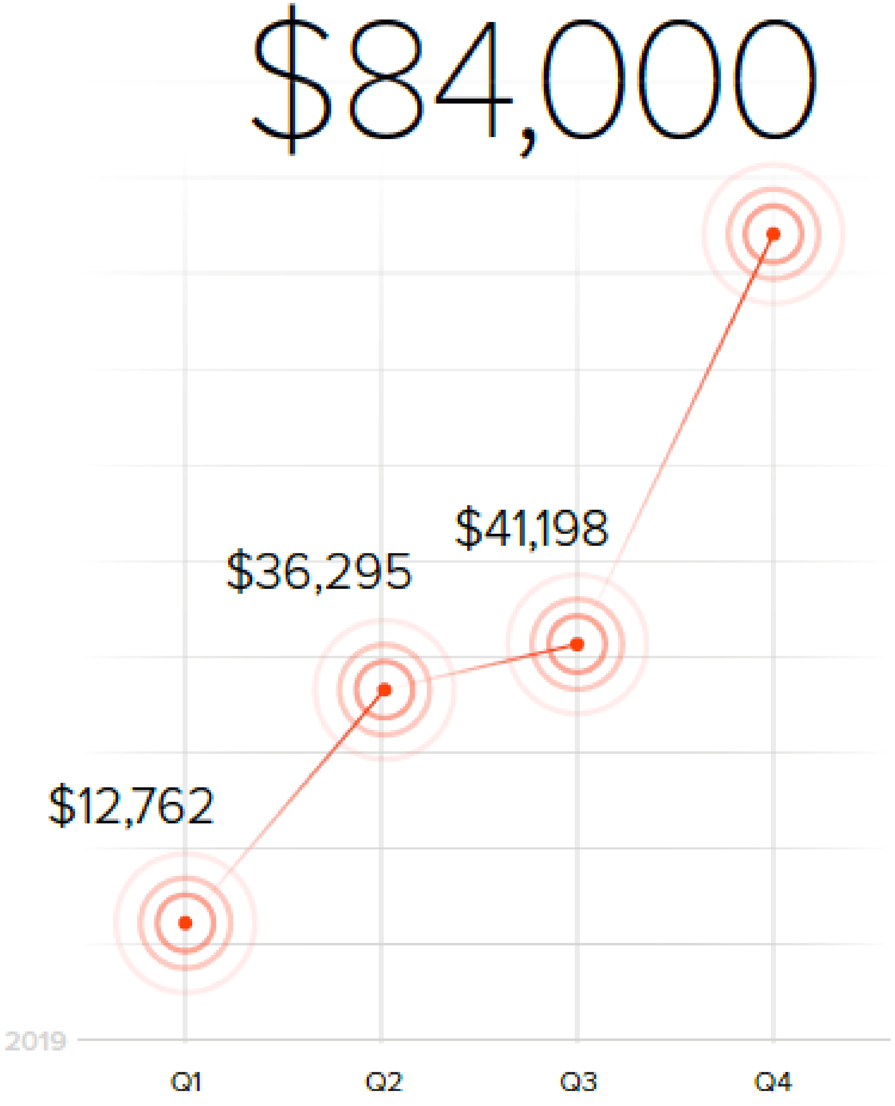
IT-Service desk
it.servicedesk@nnillersupply.co
Miller Supply

LEGEND
- ● FAKE E-MAIL ADDRESS
- ● TOO GENERIC
- ● BAD LINKS
- ● URGENCY
- ● SYNTAX & GRAMATICAL ERRORS

ClearCom
IT Solutions

Most Common Ransomware Attack Vectors Q4 2019





Average ransom amounts have exploded

ClearCom
IT Solutions

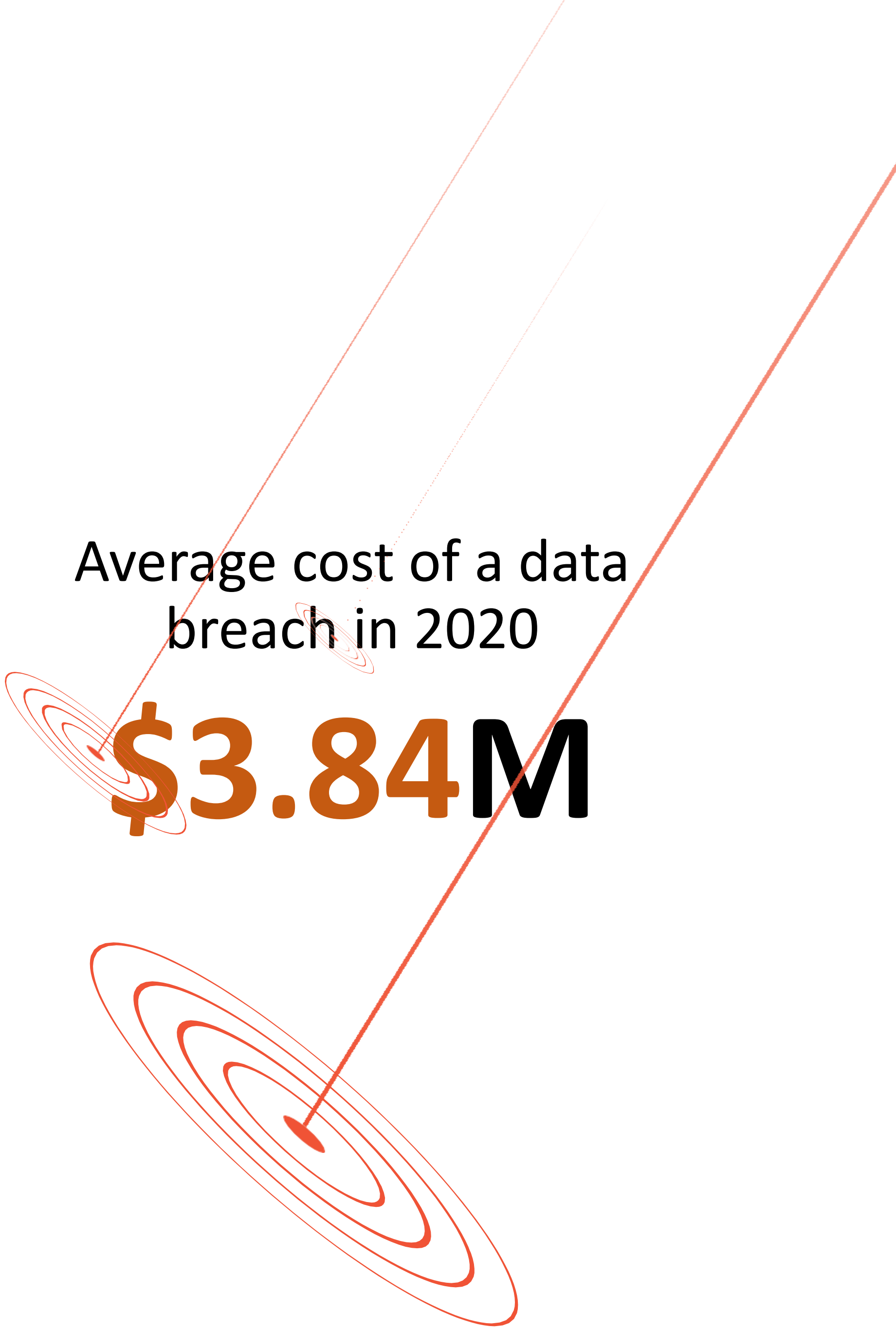
Data Exfiltration

Average time to identify and contain a breach

280 Days

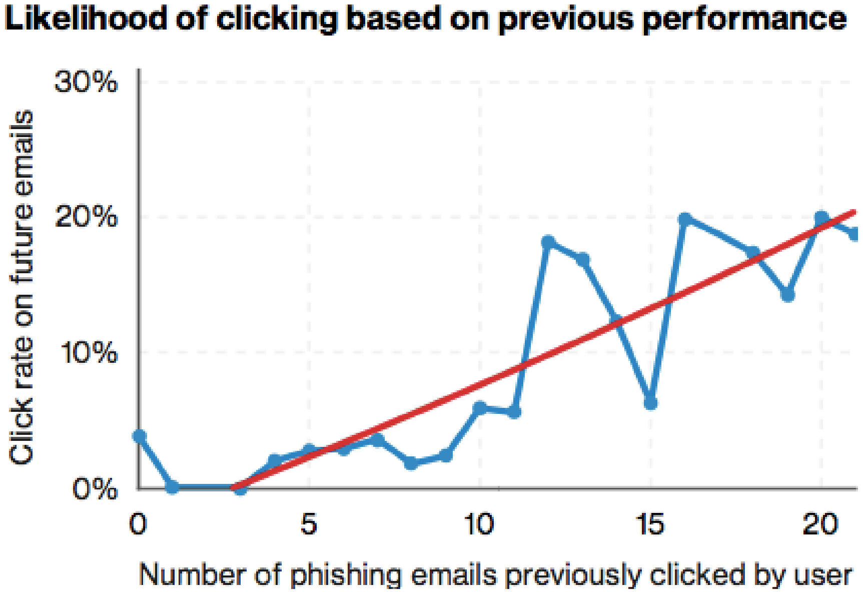
Average cost of a data breach in 2020

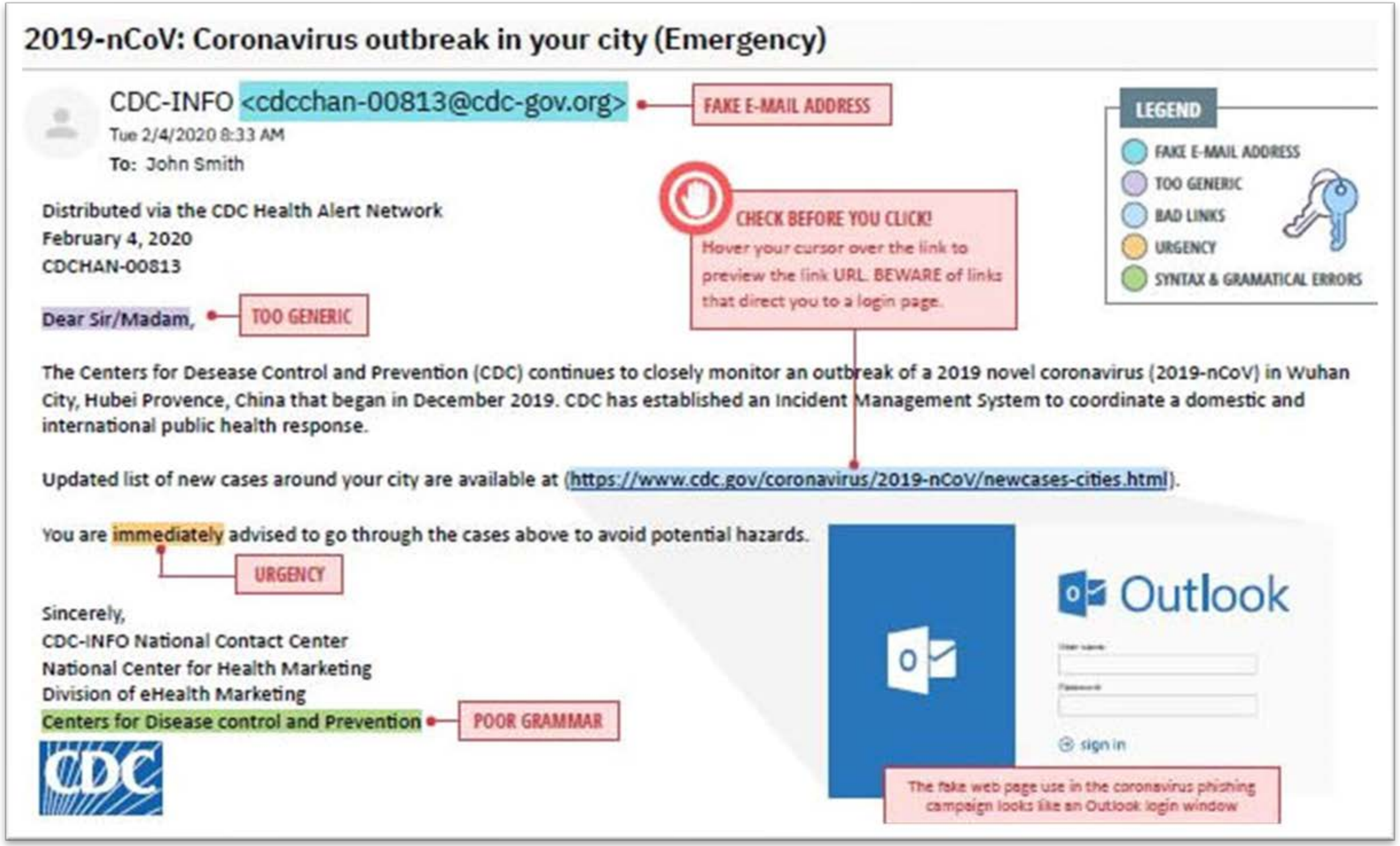
$3.84M



ClearCom
IT Solutions

URL Phishing





2019-nCoV: Coronavirus outbreak in your city (Emergency)

CDC-INFO <cdcchan-00813@cdc-gov.org>
Tue 2/4/2020 8:33 AM
To: John Smith

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00813

Dear Sir/Madam,

The Centers for Desease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Provence, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html).

You are immediately advised to go through the cases above to avoid potential hazards.

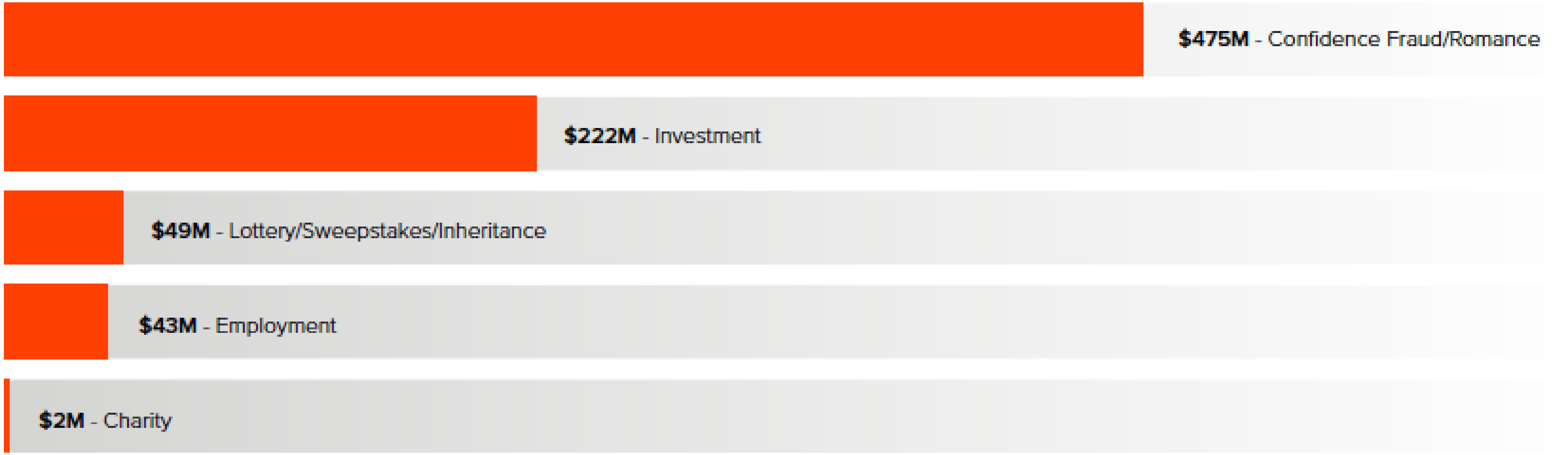
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

CHECK BEFORE YOU CLICK!
Hover your cursor over the link to preview the link URL. BEWARE of links that direct you to a login page.

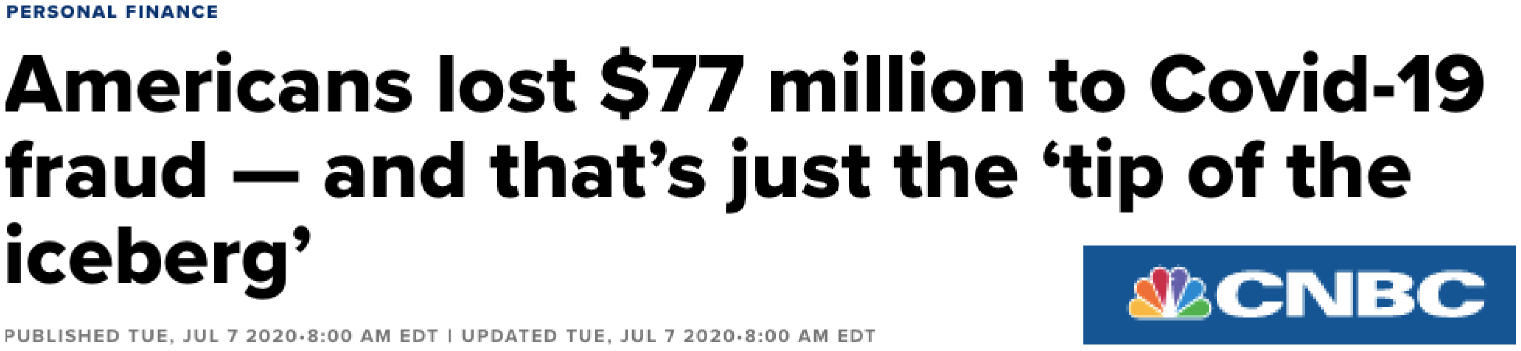
The fake web page use in the coronavirus phishing campaign looks like an Outlook login window

ClearCom
IT Solutions

Scamming



Scamming: Losses reported to the FBI in 2019



PERSONAL FINANCE

Americans lost $77 million to Covid-19 fraud — and that's just the 'tip of the iceberg'

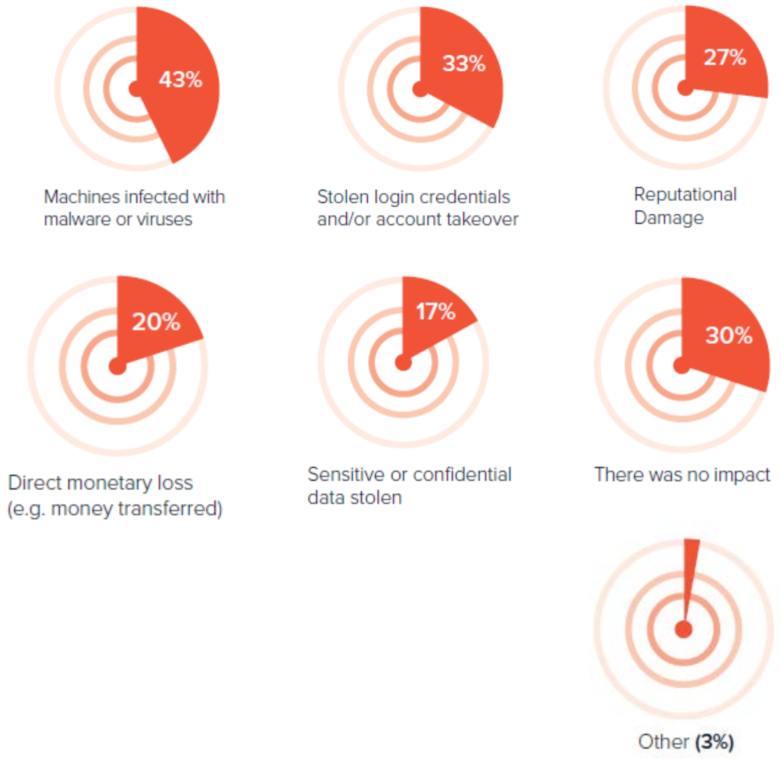
PUBLISHED TUE, JUL 7 2020·8:00 AM EDT | UPDATED TUE, JUL 7 2020·8:00 AM EDT

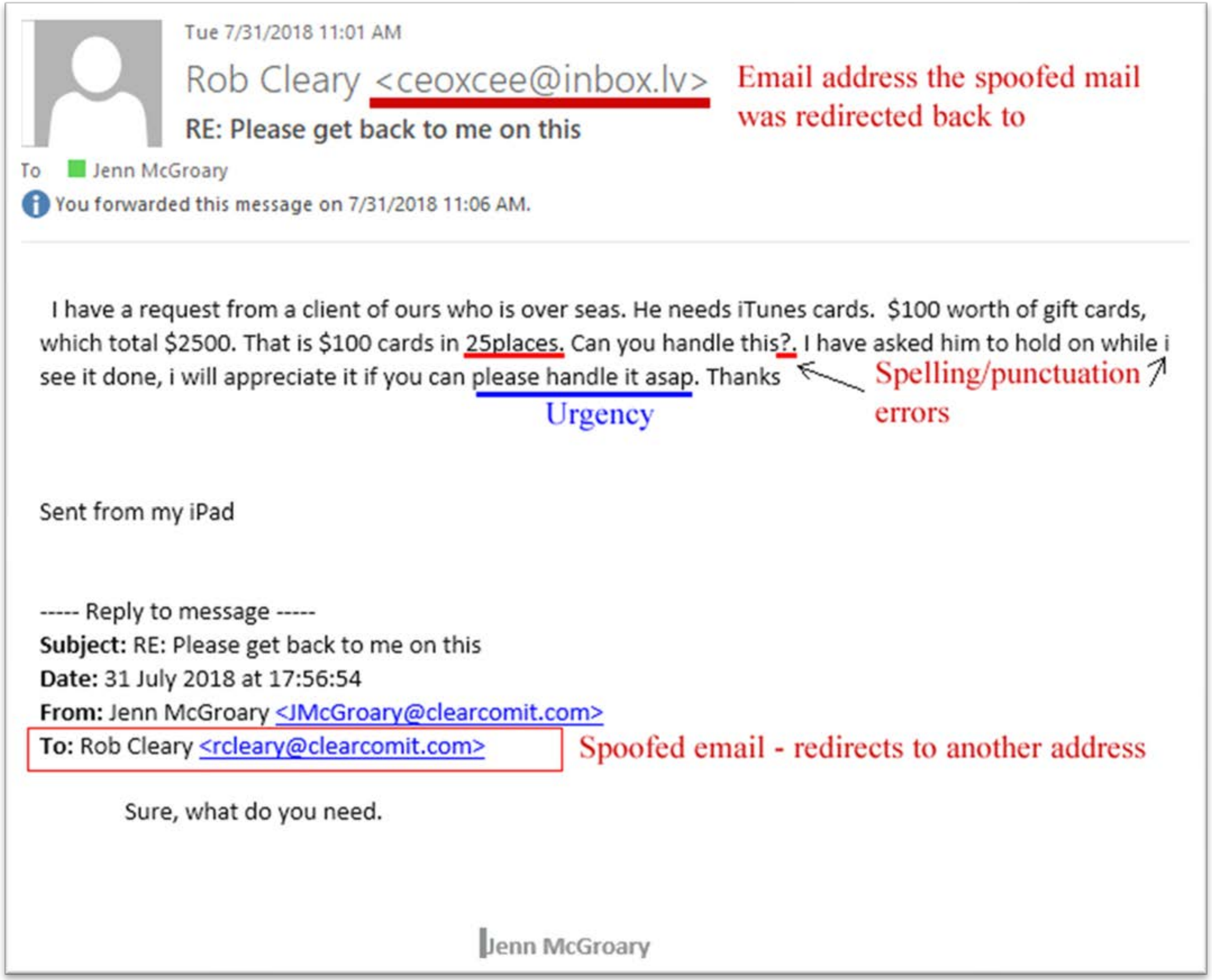
CNBC

ClearCom
IT Solutions

Spear Phishing

How businesses were affected by spear phishing attacks in 2019





Tue 7/31/2018 11:01 AM

Rob Cleary <ceoxcee@inbox.lv>

RE: Please get back to me on this

Email address the spoofed mail was redirected back to

To 🟩 Jenn McGroary

You forwarded this message on 7/31/2018 11:06 AM.

I have a request from a client of ours who is over seas. He needs iTunes cards. $100 worth of gift cards, which total $2500. That is $100 cards in 25places. Can you handle this?. I have asked him to hold on while i see it done, i will appreciate it if you can please handle it asap. Thanks

Urgency

Spelling/punctuation errors

Sent from my iPad

----- Reply to message -----
Subject: RE: Please get back to me on this
Date: 31 July 2018 at 17:56:54
From: Jenn McGroary <JMcGroary@clearcomit.com>
To: Rob Cleary <rcleary@clearcomit.com>

Spoofed email - redirects to another address

Sure, what do you need.

Jenn McGroary

ClearCom
IT Solutions

Domain Impersonation

Examples of Impersonation:

clearconit.com

cleercomit.com

cleercomit.com

clearrcomit.com

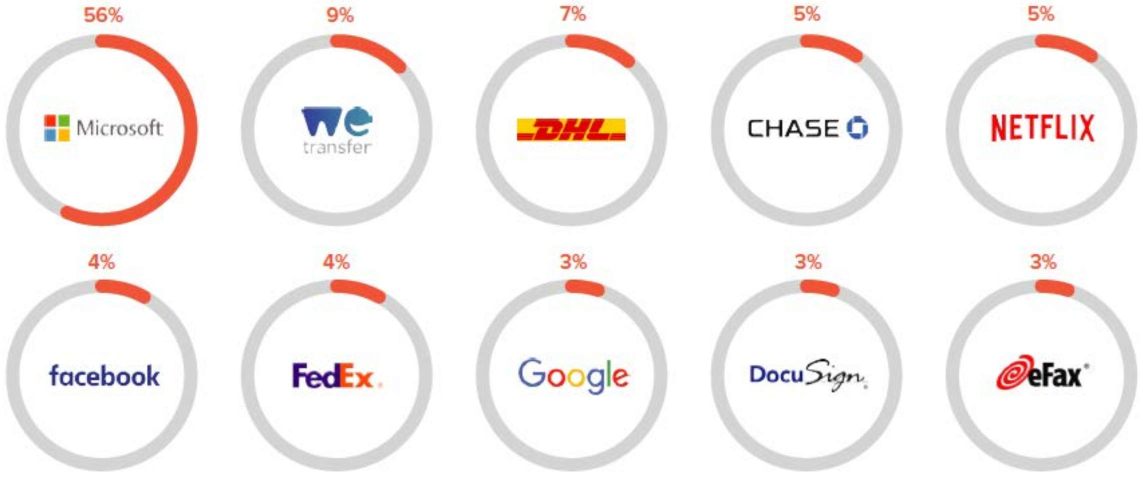
clearcomit.net

clearcomit.co

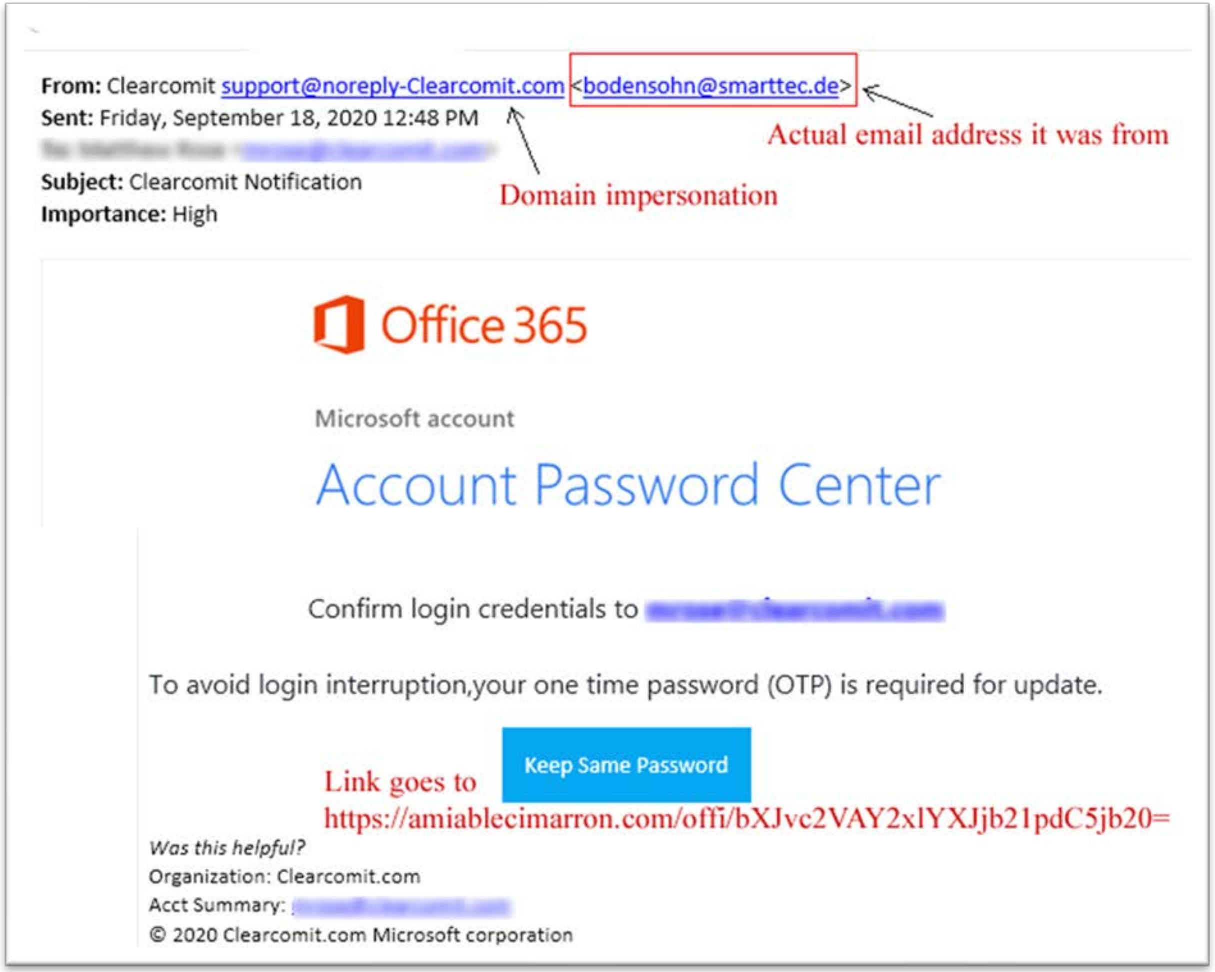
Domain impersonation increase in 2H 2019

ClearCom
IT Solutions

Brand Impersonation



Most frequently impersonated brands



From: Clearcomit support@noreply-Clearcomit.com <bodensohn@smarttec.de>
Sent: Friday, September 18, 2020 12:48 PM
[redacted]
Subject: Clearcomit Notification
Importance: High

Actual email address it was from

Domain impersonation

Office 365

Microsoft account

Account Password Center

Confirm login credentials to [redacted]

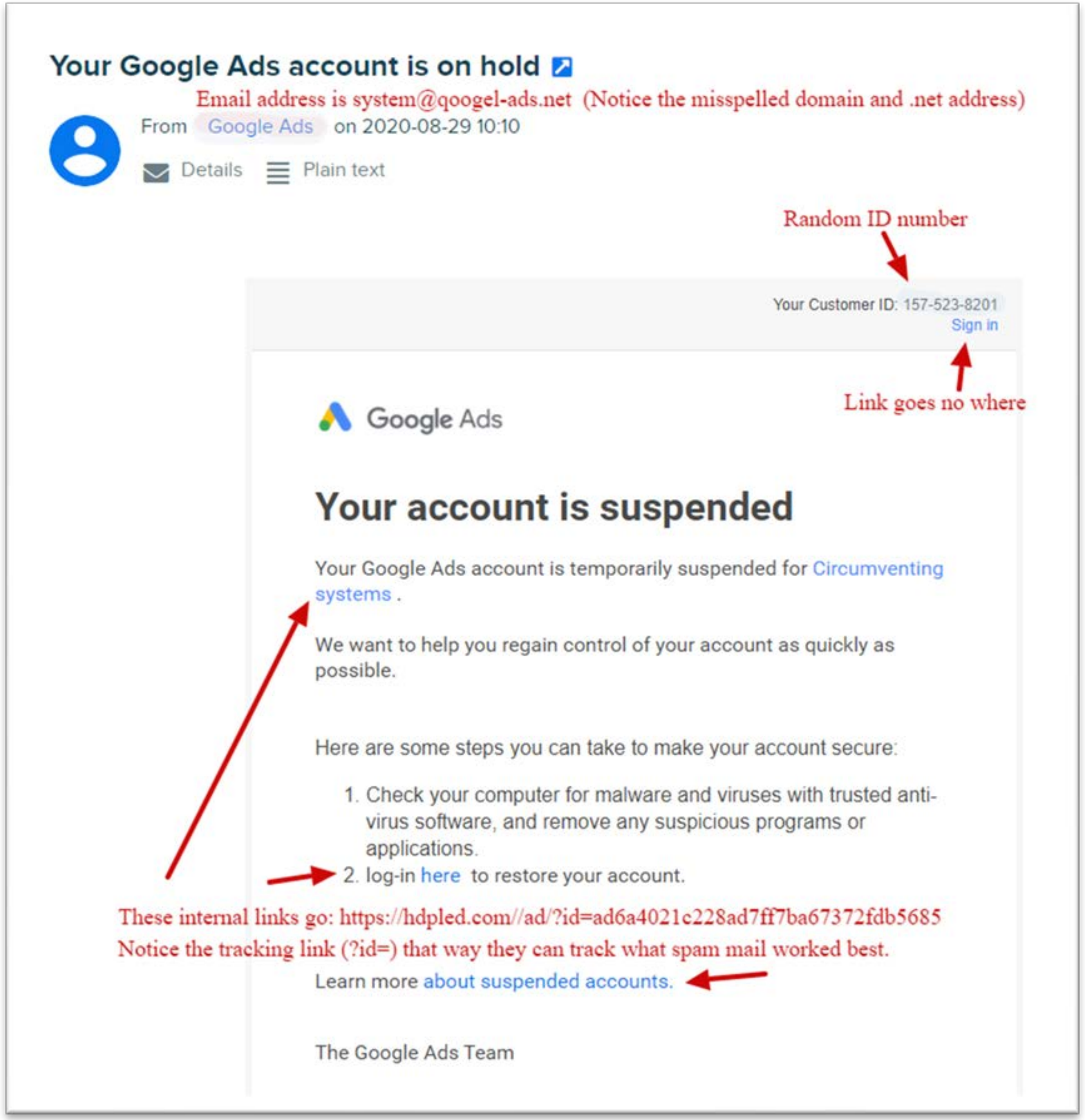
To avoid login interruption,your one time password (OTP) is required for update.

Keep Same Password

Link goes to https://amiablecimarron.com/offi/bXJvc2VAY2xlYXJjb21pdC5jb20=

Was this helpful?
Organization: Clearcomit.com
Acct Summary: [redacted]
© 2020 Clearcomit.com Microsoft corporation

ClearCom
IT Solutions



Your Google Ads account is on hold

Email address is system@qoogel-ads.net (Notice the misspelled domain and .net address)

From Google Ads on 2020-08-29 10:10

Details   Plain text

Random ID number

Your Customer ID: 157-523-8201
Sign in

Link goes no where

Google Ads

Your account is suspended

Your Google Ads account is temporarily suspended for Circumventing systems .

We want to help you regain control of your account as quickly as possible.

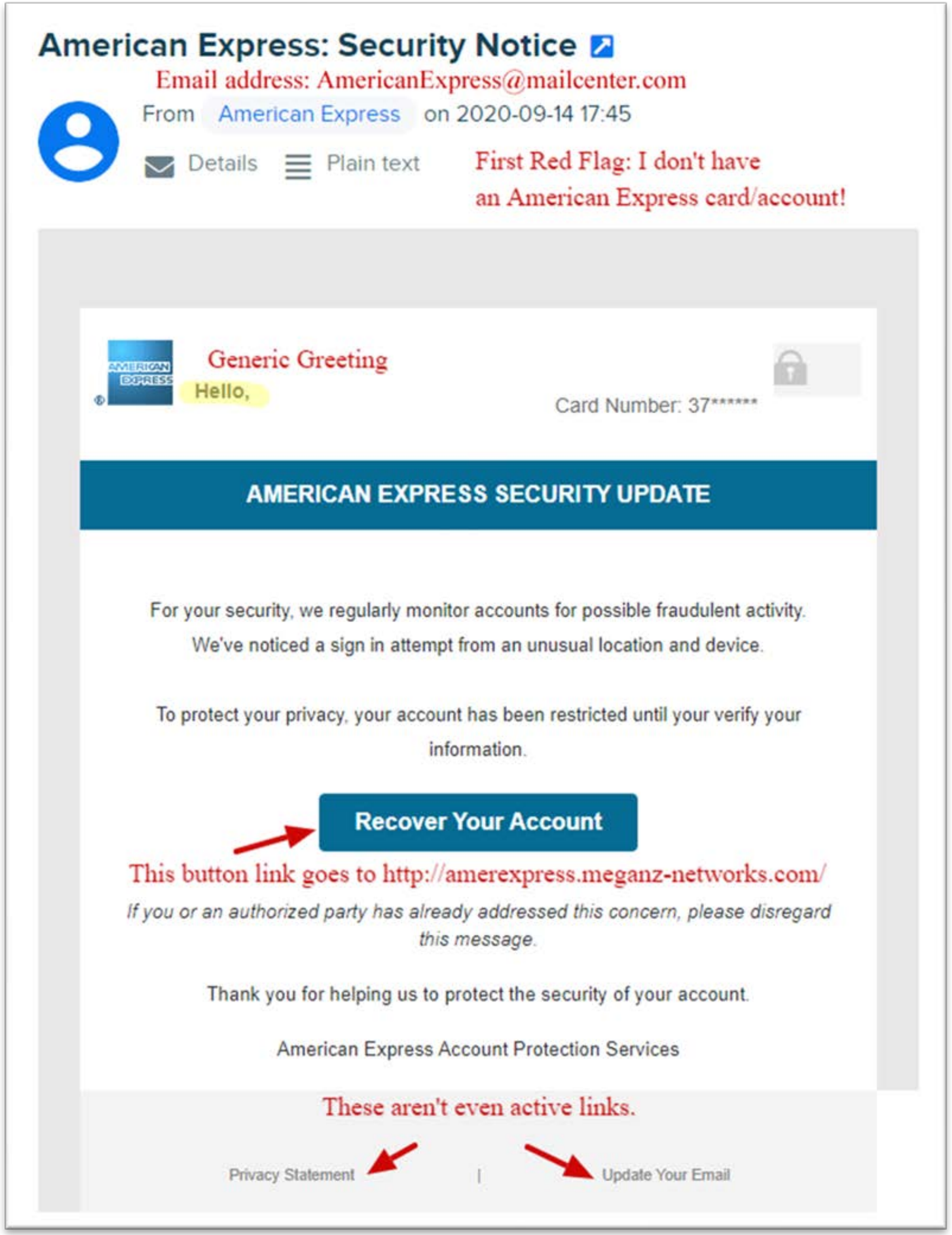
Here are some steps you can take to make your account secure:

1. Check your computer for malware and viruses with trusted anti-virus software, and remove any suspicious programs or applications.
2. log-in here to restore your account.

These internal links go: https://hdpled.com//ad/?id=ad6a4021c228ad7ff7ba67372fdb5685
Notice the tracking link (?id=) that way they can track what spam mail worked best.

Learn more about suspended accounts.

The Google Ads Team



American Express: Security Notice

Email address: AmericanExpress@mailcenter.com

From American Express on 2020-09-14 17:45

Details   Plain text

First Red Flag: I don't have
an American Express card/account!

Generic Greeting

Hello,

Card Number: 37******

AMERICAN EXPRESS SECURITY UPDATE

For your security, we regularly monitor accounts for possible fraudulent activity. We've noticed a sign in attempt from an unusual location and device.

To protect your privacy, your account has been restricted until your verify your information.

Recover Your Account

This button link goes to http://amerexpress.meganz-networks.com/

If you or an authorized party has already addressed this concern, please disregard this message.

Thank you for helping us to protect the security of your account.

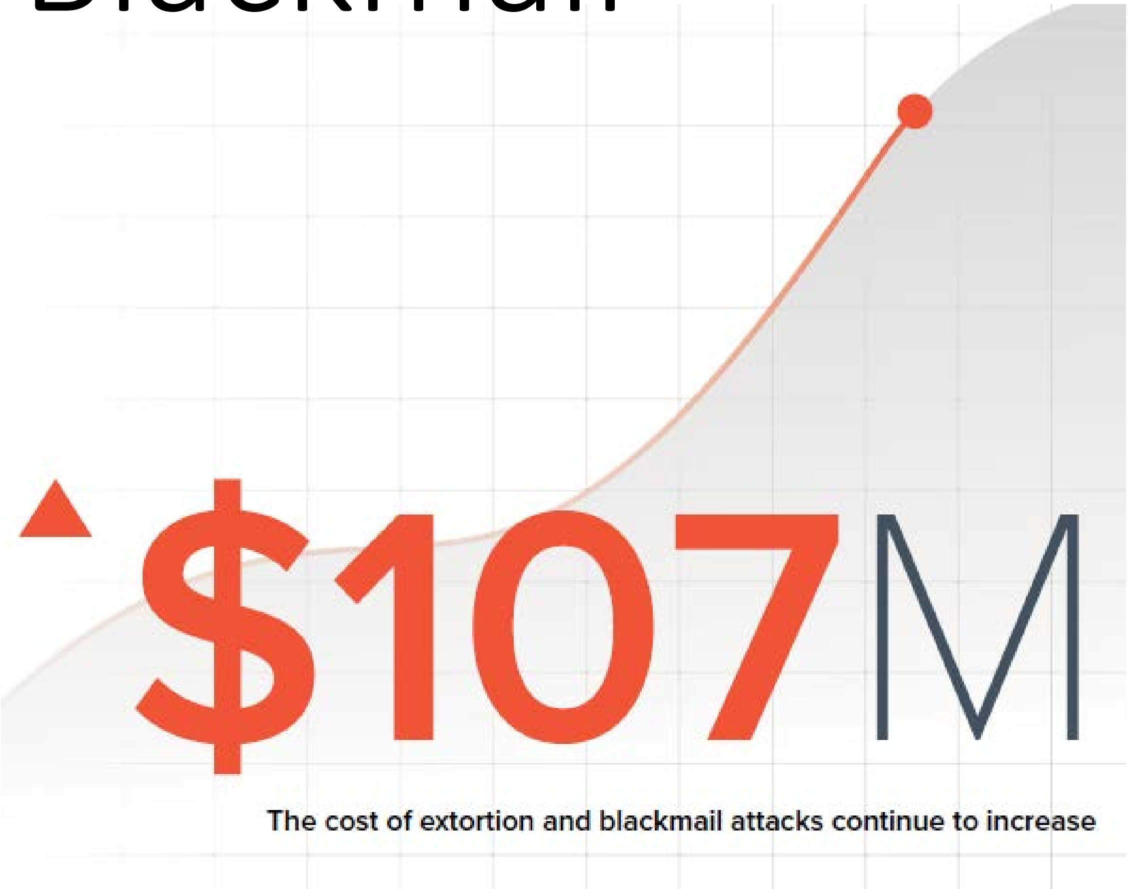
American Express Account Protection Services

These aren't even active links.

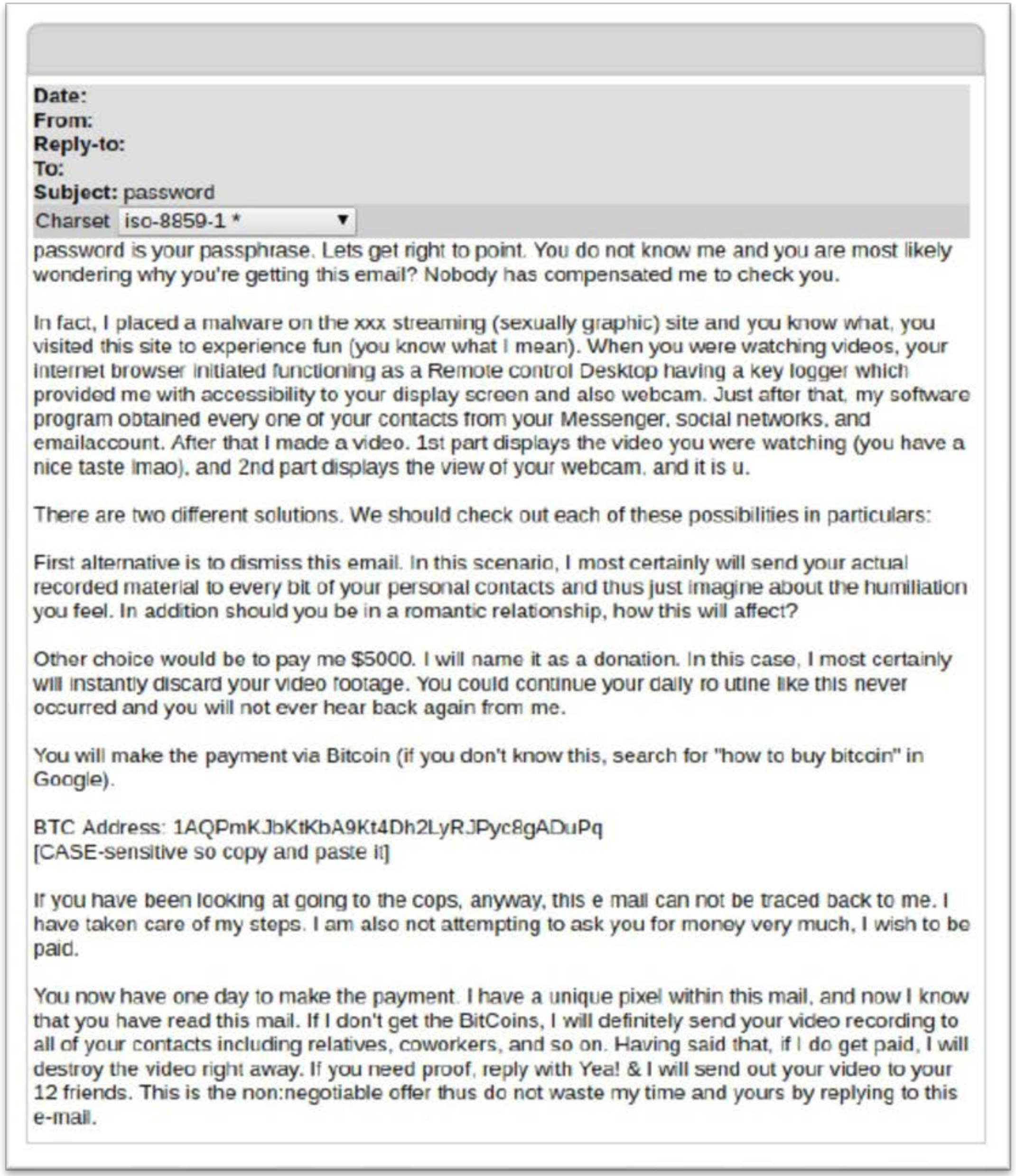
Privacy Statement | Update Your Email

ClearCom
IT Solutions

Blackmail



The cost of extortion and blackmail attacks continue to increase



Date:
From:
Reply-to:
To:
Subject: password
Charset iso-8859-1 * ▼

password is your passphrase. Lets get right to point. You do not know me and you are most likely wondering why you're getting this email? Nobody has compensated me to check you.

In fact, I placed a malware on the xxx streaming (sexually graphic) site and you know what, you visited this site to experience fun (you know what I mean). When you were watching videos, your internet browser initiated functioning as a Remote control Desktop having a key logger which provided me with accessibility to your display screen and also webcam. Just after that, my software program obtained every one of your contacts from your Messenger, social networks, and emailaccount. After that I made a video. 1st part displays the video you were watching (you have a nice taste lmao), and 2nd part displays the view of your webcam, and it is u.

There are two different solutions. We should check out each of these possibilities in particulars:

First alternative is to dismiss this email. In this scenario, I most certainly will send your actual recorded material to every bit of your personal contacts and thus just imagine about the humiliation you feel. In addition should you be in a romantic relationship, how this will affect?

Other choice would be to pay me $5000. I will name it as a donation. In this case, I most certainly will instantly discard your video footage. You could continue your daily ro utine like this never occurred and you will not ever hear back again from me.

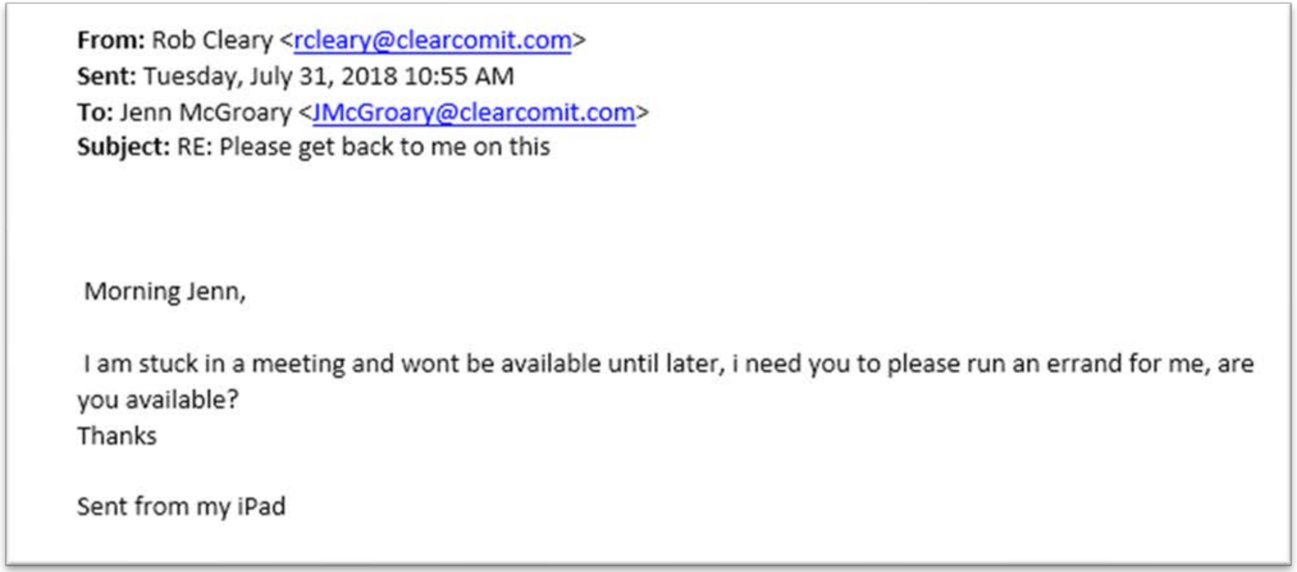
You will make the payment via Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1AQPmKJbKtKbA9Kt4Dh2LyRJPyc8gADuPq
[CASE-sensitive so copy and paste it]

If you have been looking at going to the cops, anyway, this e mail can not be traced back to me. I have taken care of my steps. I am also not attempting to ask you for money very much, I wish to be paid.

You now have one day to make the payment. I have a unique pixel within this mail, and now I know that you have read this mail. If I don't get the BitCoins, I will definitely send your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I do get paid, I will destroy the video right away. If you need proof, reply with Yea! & I will send out your video to your 12 friends. This is the non:negotiable offer thus do not waste my time and yours by replying to this e-mail.

Business Email Compromise

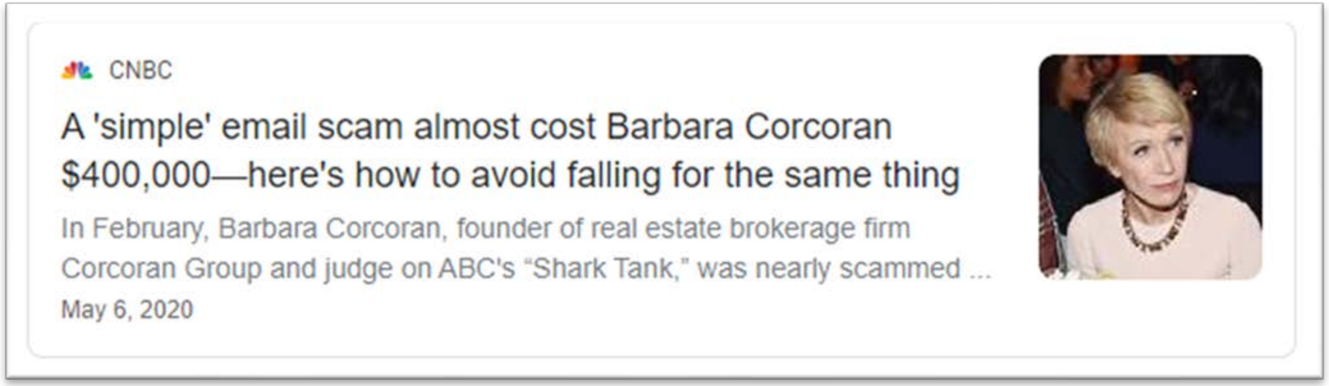


From: Rob Cleary <rcleary@clearcomit.com>
Sent: Tuesday, July 31, 2018 10:55 AM
To: Jenn McGroary <JMcGroary@clearcomit.com>
Subject: RE: Please get back to me on this

Morning Jenn,

I am stuck in a meeting and wont be available until later, i need you to please run an errand for me, are you available?
Thanks

Sent from my iPad



CNBC

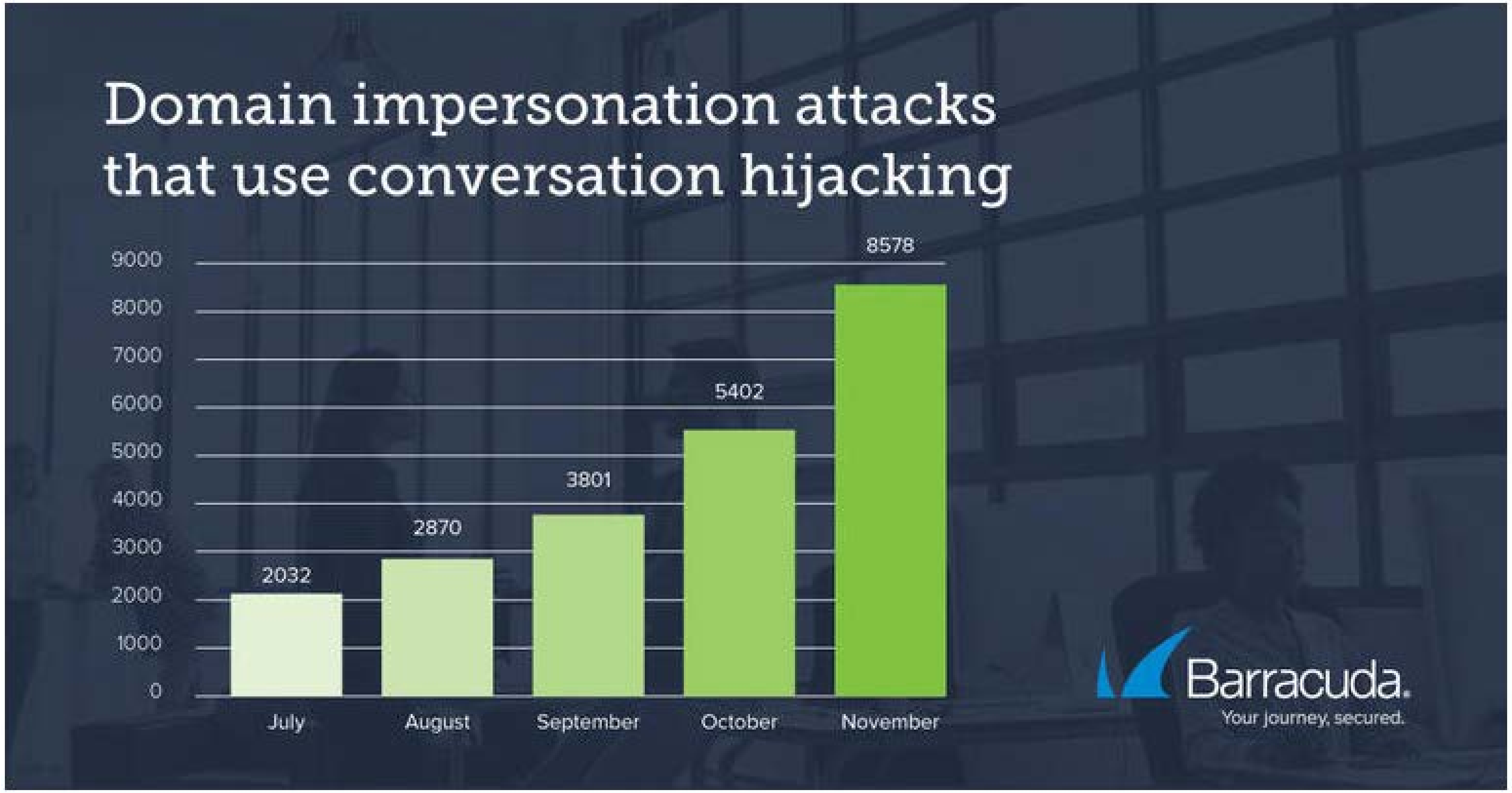
A 'simple' email scam almost cost Barbara Corcoran $400,000—here's how to avoid falling for the same thing

In February, Barbara Corcoran, founder of real estate brokerage firm Corcoran Group and judge on ABC's "Shark Tank," was nearly scammed ...

May 6, 2020

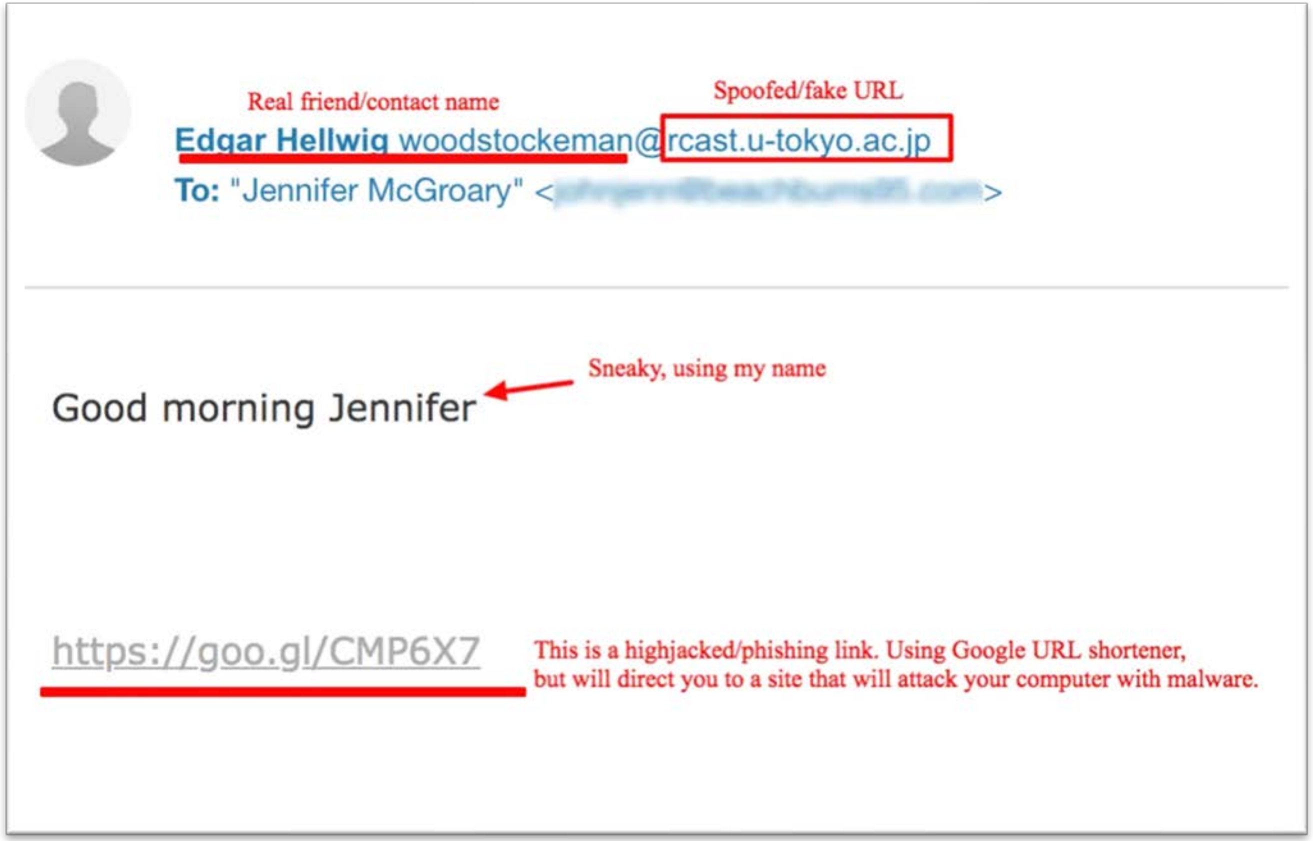
ClearCom
IT Solutions

Conversation Hijacking



ClearCom
IT Solutions

Lateral Phishing



Real friend/contact name

Spoofed/fake URL

Edgar Hellwig woodstockeman@rcast.u-tokyo.ac.jp

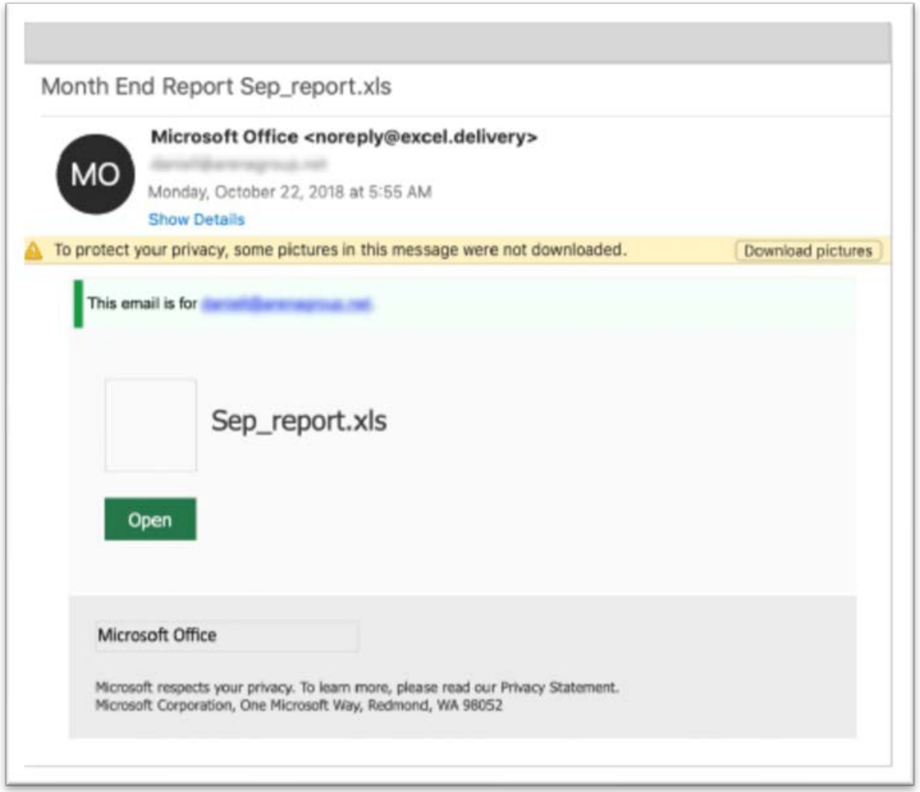
To: "Jennifer McGroary" <[redacted]>

Good morning Jennifer

Sneaky, using my name

https://goo.gl/CMP6X7

This is a highjacked/phishing link. Using Google URL shortener, but will direct you to a site that will attack your computer with malware.



Month End Report Sep_report.xls

Microsoft Office <noreply@excel.delivery>

[redacted]

Monday, October 22, 2018 at 5:55 AM

Show Details

⚠ To protect your privacy, some pictures in this message were not downloaded. Download pictures

This email is for [redacted]

Sep_report.xls

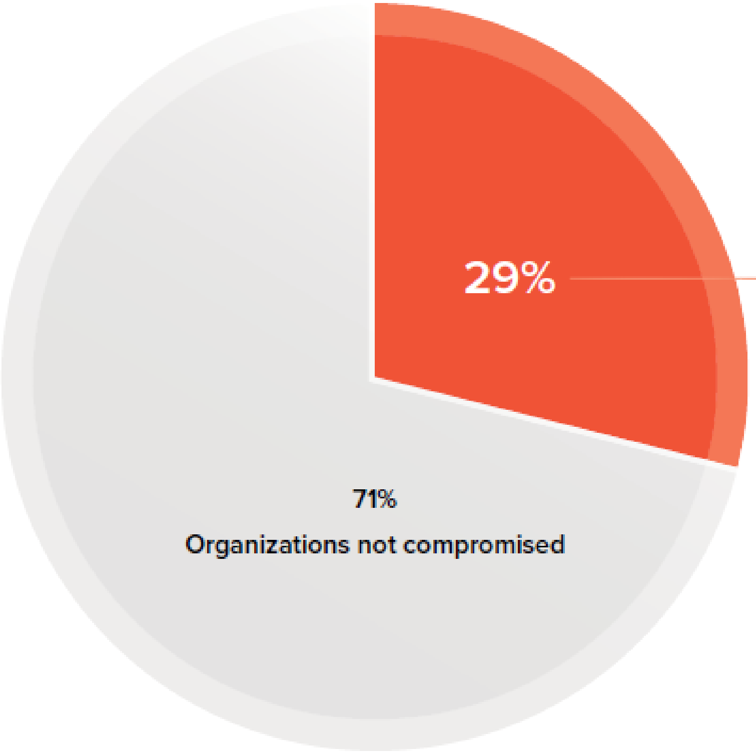
Open

Microsoft Office

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

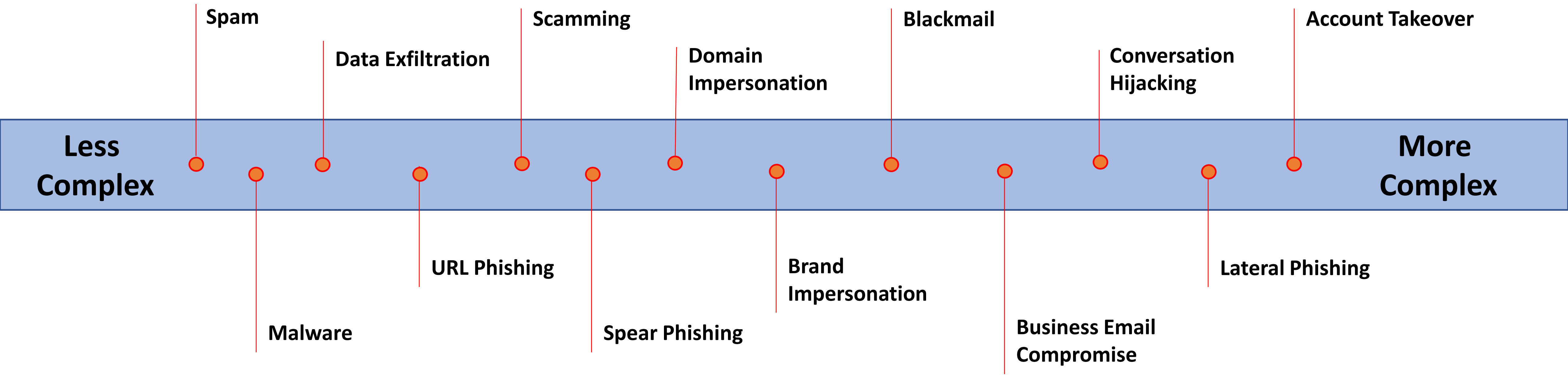
ClearCom
IT Solutions

Account Takeover



of organizations had their **Microsoft Office 365 accounts compromised in one month**

13 Different Types of Threats



Less Complex

Spam

Malware

Data Exfiltration

URL Phishing

Scamming

Spear Phishing

Domain Impersonation

Brand Impersonation

Blackmail

Business Email Compromise

Conversation Hijacking

Lateral Phishing

Account Takeover

More Complex

ClearCom IT Solutions

ClearCom IT Advanced Security Bundle

Enhanced Anti-Virus,
Threat Detection & Encryption

Enhanced Spam Filter

End User Phishing Training
& Dark Web Monitoring

ClearCom
IT Solutions

Who is this for

- Values increased security of company data and reputation
- Wants peace of mind that threats are minimized

Who is this NOT for

- OK with basic security for company data
- Only has 1 or 2 team members and you don’t click on any email links
- Not concerned about cyber attacks.

ClearCom
IT Solutions

Next Steps

- Click on the button below this video where you'll be directed to www.clearcomit.com/email15
- Click the big blue "book now" button on the page.
- In the box that opens, select the date/time that works best for your schedule.
- Include your best phone number so we can reach you at the appointed date/time.
- Include your business email domain so we can run your complementary Dark Web Report.
- Check your inbox for an email with a calendar invite. Make sure you click on that calendar file to add the appointment to your calendar.

To talk ASAP, you can give us a call directly at 508-205-1114

ClearCom
IT Solutions

ClearCom
IT Solutions