June 2020

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Are You Prepared? COVID 19 and Cybersecurity

©2018 CliftonLarsonAllen LLP

Create Opportunities

We promise to know you and help you.

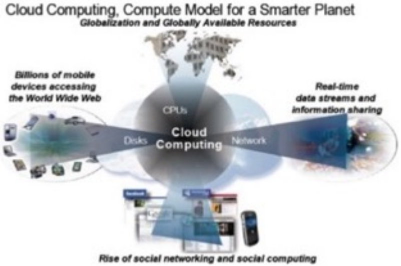
C:\whoami
> m0th_man

©2018 CliftonLarsonAllen LLP

- “Professional Student”
- Science Teacher / Self Taught Computer Guy
- IT Consultant - Project Manager → IT Staff/Help Desk → Hacker
- Assistant Scout Master (Boy Scouts)
- Boys Scouts Motto: Be Prepared – Are you prepared?

Raise Your Hand If…

Body Gateway
PAN
WAN
Care Server
Internet
Internet
ADSL
PAN
PAN
Off-body sensors

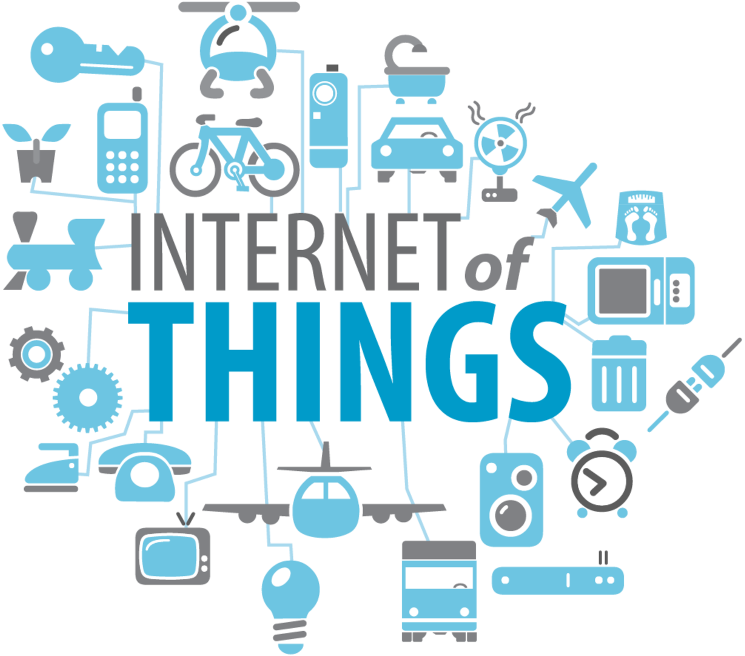

Cloud Computing, Compute Model for a Smarter Planet
Globalization and Globally Available Resources
Billions of mobile devices accessing the World Wide Web
Real-time data streams and information sharing
CPUs
Disks
Cloud Computing
Network
Rise of social networking and social computing

©2018 CliftonLarsonAllen LLP

Everything Can Talk to Everything….

- Security cameras
- Garage door
- Home thermostat
- Cable TV remote
- Sleep number bed
- “Hey Siri, what’s my balance?”
- Roomba

➢ **“Presence”**



©2018 CliftonLarsonAllen LLP

Sun Tzu:

“Know your enemy and know yourself and you can fight a hundred battles without disaster”

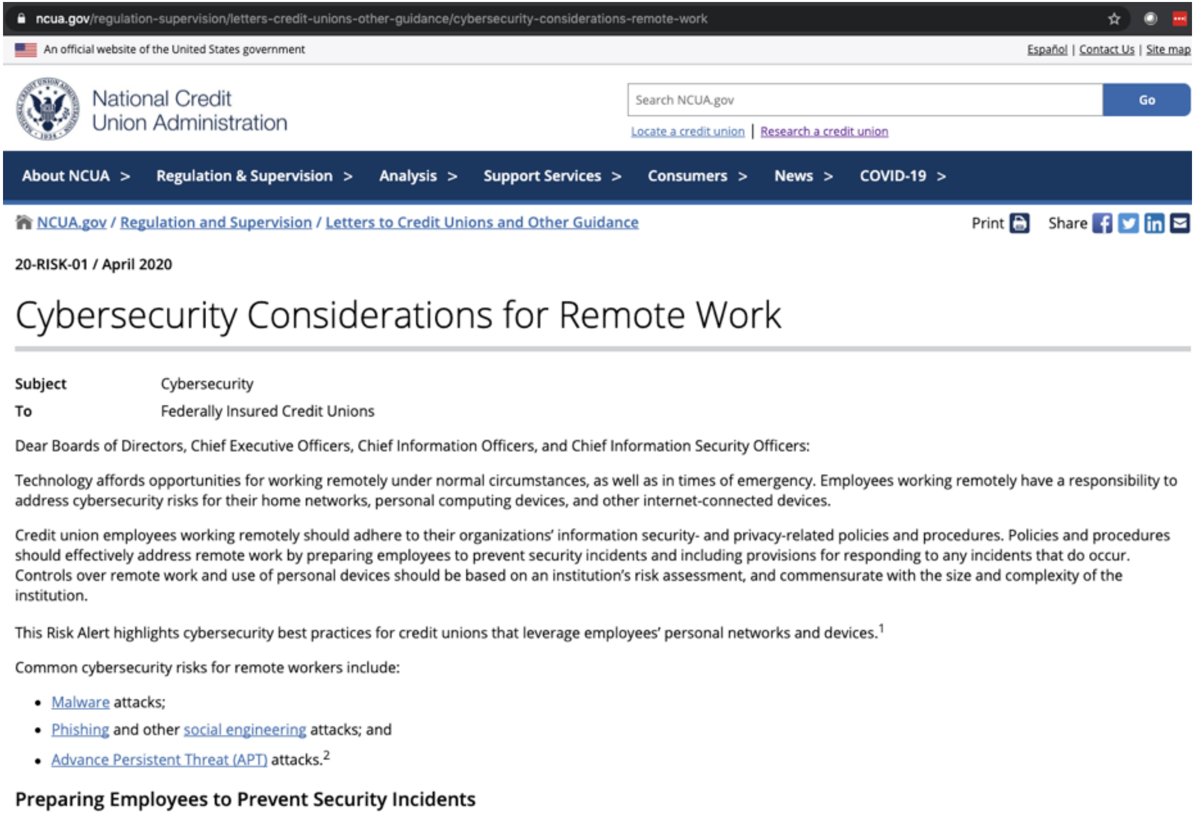
The Current State of Cybercrime

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

©2018 CliftonLarsonAllen LLP

Risk Landscape



ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/cybersecurity-considerations-remote-work
An official website of the United States government
Español | Contact Us | Site map
National Credit Union Administration
Search NCUA.gov
Go
Locate a credit union | Research a credit union
About NCUA >
Regulation & Supervision >
Analysis >
Support Services >
Consumers >
News >
COVID-19 >
NCUA.gov / Regulation and Supervision / Letters to Credit Unions and Other Guidance
Print
Share

20-RISK-01 / April 2020

Cybersecurity Considerations for Remote Work

Subject Cybersecurity

To Federally Insured Credit Unions

Dear Boards of Directors, Chief Executive Officers, Chief Information Officers, and Chief Information Security Officers:

Technology affords opportunities for working remotely under normal circumstances, as well as in times of emergency. Employees working remotely have a responsibility to address cybersecurity risks for their home networks, personal computing devices, and other internet-connected devices.

Credit union employees working remotely should adhere to their organizations' information security- and privacy-related policies and procedures. Policies and procedures should effectively address remote work by preparing employees to prevent security incidents and including provisions for responding to any incidents that do occur. Controls over remote work and use of personal devices should be based on an institution's risk assessment, and commensurate with the size and complexity of the institution.

This Risk Alert highlights cybersecurity best practices for credit unions that leverage employees' personal networks and devices.[1]

Common cybersecurity risks for remote workers include:

- Malware attacks;
- Phishing and other social engineering attacks; and
- Advance Persistent Threat (APT) attacks.[2]

Preparing Employees to Prevent Security Incidents

©2018 CliftonLarsonAllen LLP

Risk Landscape

©2018 CliftonLarsonAllen LLP

Remote Workforce

- Remote access vulnerabilities
- Impersonation of employees
- Personal devices
- Direct application access

Phishing Attacks

- Not just email, SMS
- Promises of assistance related to the pandemic
- Offer medical supplies
- Immediate cures

Malware

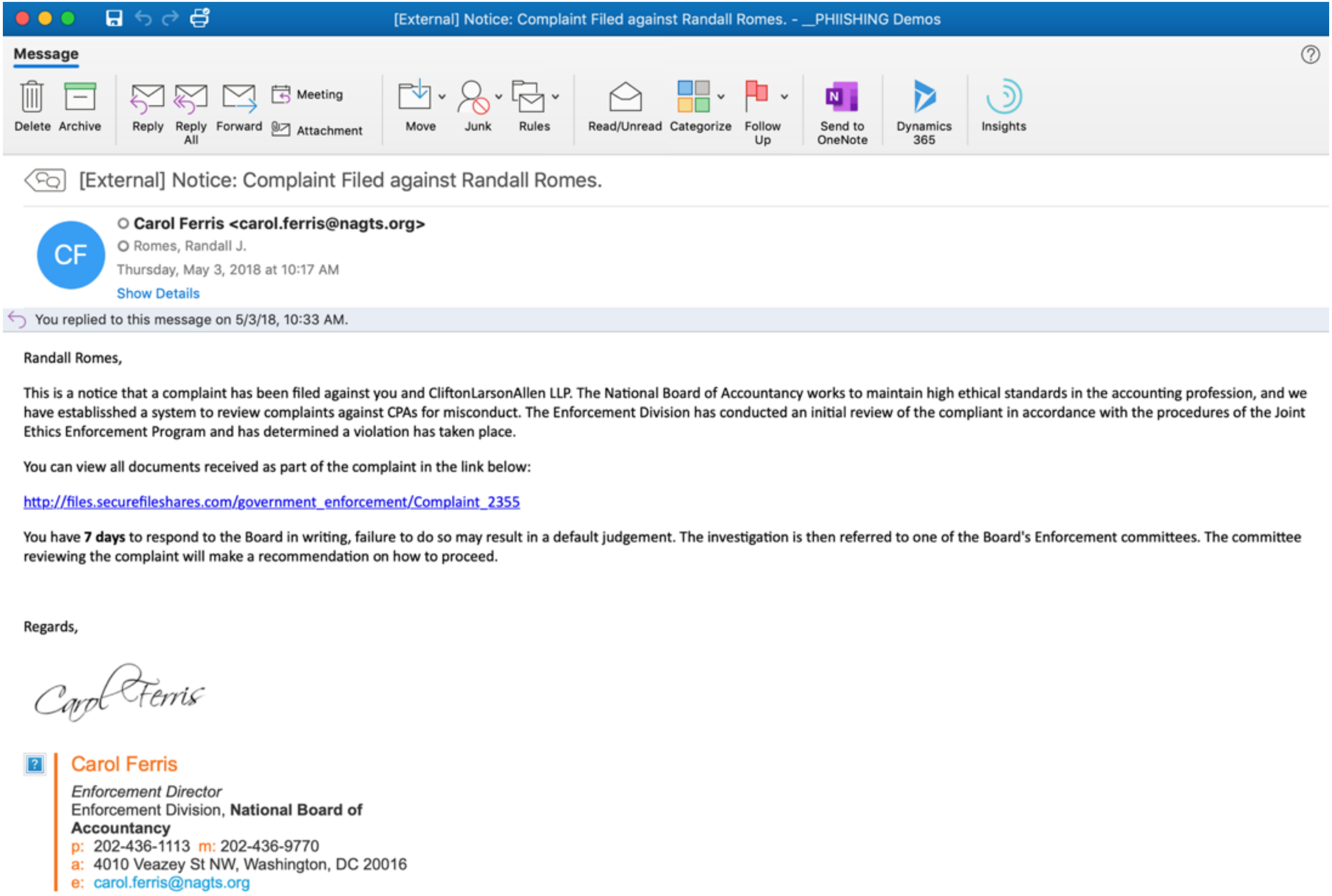
- Corona Virus Map malware
- Free applications to help
- Anti Virus/ malware scanning and definition updates

Cybercrime and Black Market Economies

- Black market economy to support cyber fraud
  - Business models and specialization

- Most common cyber fraud scenarios we see affecting our clients
  - Theft of credit card information
  - Theft of Credentials & Account take overs
  - Theft of PII and PFI
  - Ransomware and Interference w/ Operations
  - Email phishing is still a root cause in 90% of breaches

©2018 CliftonLarsonAllen LLP



[External] Notice: Complaint Filed against Randall Romes.

○ **Carol Ferris <carol.ferris@nagts.org>**
○ Romes, Randall J.
Thursday, May 3, 2018 at 10:17 AM
Show Details

You replied to this message on 5/3/18, 10:33 AM.

Randall Romes,

This is a notice that a complaint has been filed against you and CliftonLarsonAllen LLP. The National Board of Accountancy works to maintain high ethical standards in the accounting profession, and we have establisshed a system to review complaints against CPAs for misconduct. The Enforcement Division has conducted an initial review of the compliant in accordance with the procedures of the Joint Ethics Enforcement Program and has determined a violation has taken place.

You can view all documents received as part of the complaint in the link below:

http://files.securefileshares.com/government_enforcement/Complaint_2355

You have **7 days** to respond to the Board in writing, failure to do so may result in a default judgement. The investigation is then referred to one of the Board's Enforcement committees. The committee reviewing the complaint will make a recommendation on how to proceed.

Regards,

Carol Ferris

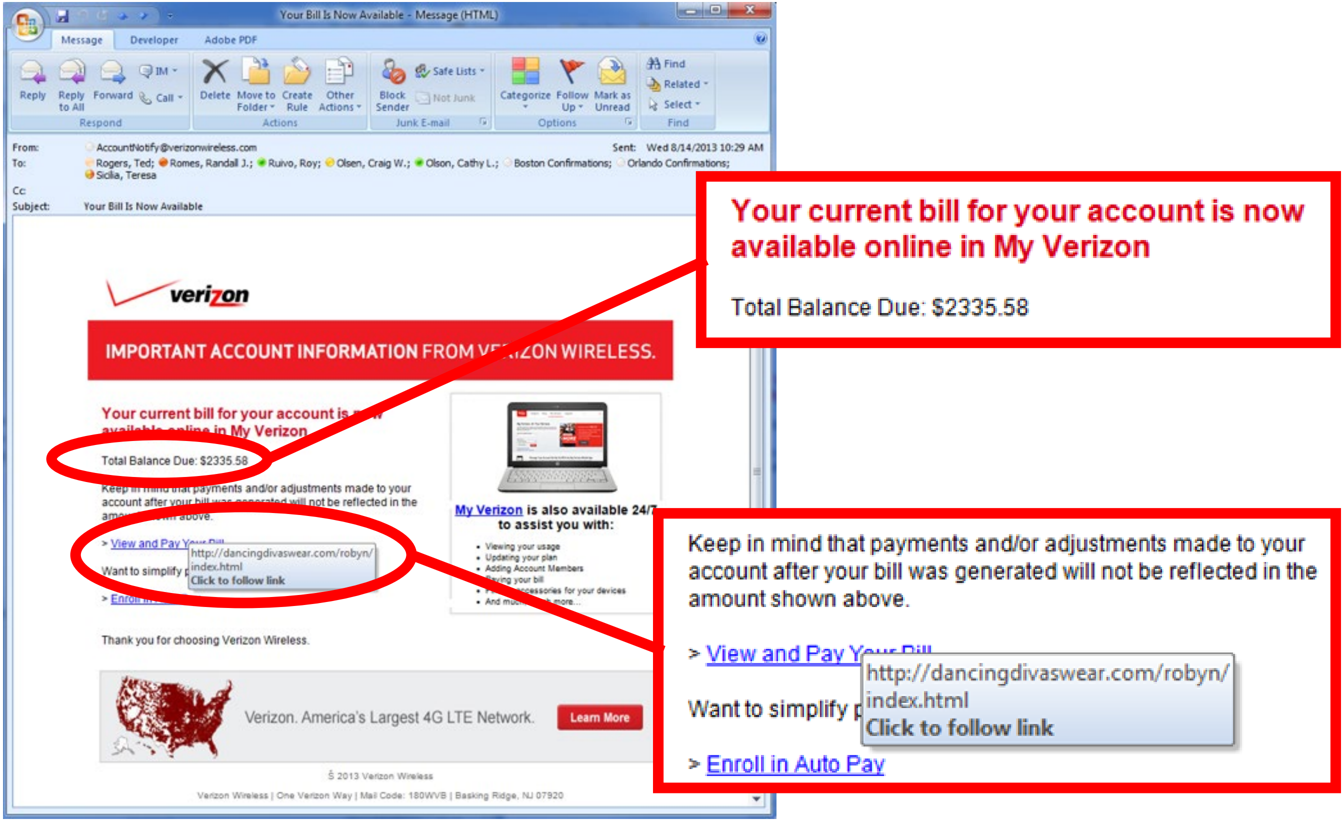
Carol Ferris

Enforcement Director
Enforcement Division, **National Board of Accountancy**
p: 202-436-1113 m: 202-436-9770
a: 4010 Veazey St NW, Washington, DC 20016
e: carol.ferris@nagts.org

©2018 CliftonLarsonAllen LLP

Phishing?

©2018 CliftonLarsonAllen LLP



From: AccountNotify@verizonwireless.com

Sent: Wed 8/14/2013 10:29 AM

To: Rogers, Ted; Romes, Randall J.; Ruivo, Roy; Olsen, Craig W.; Olson, Cathy L.; Boston Confirmations; Orlando Confirmations; Sicilia, Teresa

Cc:

Subject: Your Bill Is Now Available

IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

Your current bill for your account is now available online in My Verizon

Total Balance Due: $2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> View and Pay Your Bill

http://dancingdivaswear.com/robyn/index.html
Click to follow link

Want to simplify p

> Enroll in Auto Pay

My Verizon is also available 24/7 to assist you with:

- Viewing your usage
- Updating your plan
- Adding Account Members
- Paying your bill
- P accessories for your devices
- And much more...

Thank you for choosing Verizon Wireless.

Verizon. America's Largest 4G LTE Network.

Š 2013 Verizon Wireless

Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07920

Your current bill for your account is now available online in My Verizon

Total Balance Due: $2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> View and Pay Your Bill

http://dancingdivaswear.com/robyn/index.html
Click to follow link

Want to simplify p

> Enroll in Auto Pay

COVID “Opportunities”

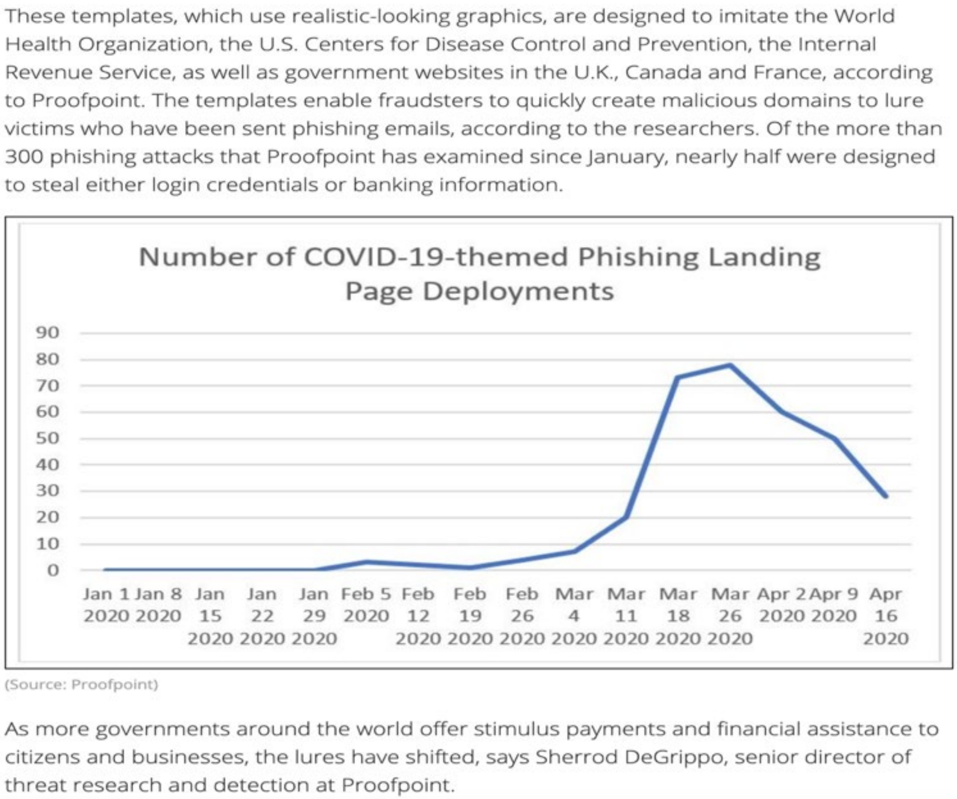
1. Virus/health related news
2. Remote Work force
3. Re-opening of businesses
4. SBA funding
5. PPP programs
6. Political news

©2018 CliftonLarsonAllen LLP

COVID "Opportunities"

Most breaches have a root cause in some form of Phishing

What is "Spear Phishing"



These templates, which use realistic-looking graphics, are designed to imitate the World Health Organization, the U.S. Centers for Disease Control and Prevention, the Internal Revenue Service, as well as government websites in the U.K., Canada and France, according to Proofpoint. The templates enable fraudsters to quickly create malicious domains to lure victims who have been sent phishing emails, according to the researchers. Of the more than 300 phishing attacks that Proofpoint has examined since January, nearly half were designed to steal either login credentials or banking information.

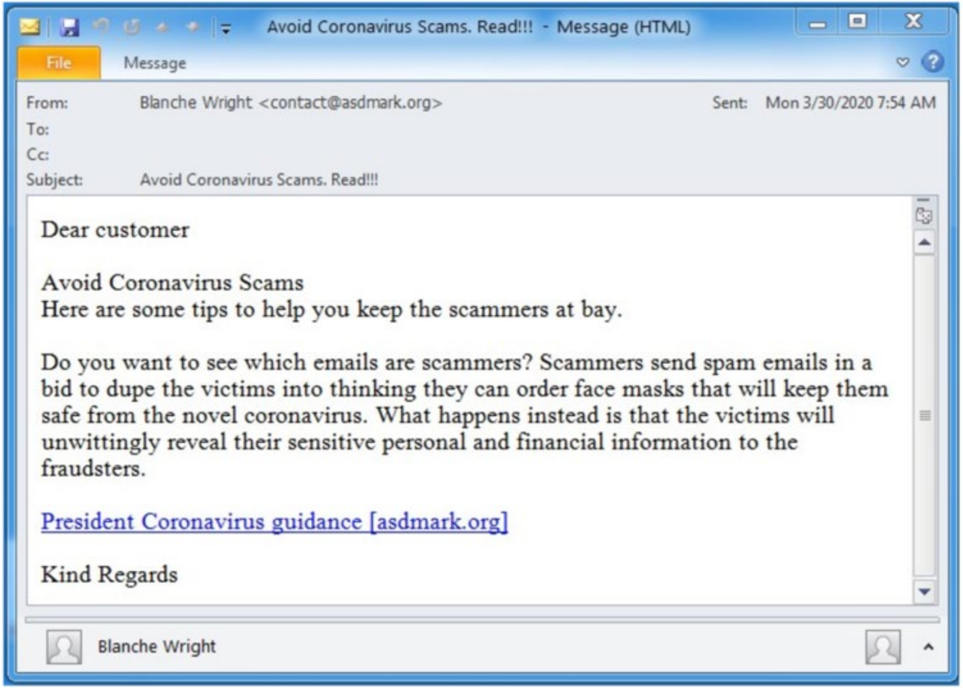
Number of COVID-19-themed Phishing Landing Page Deployments

(Source: Proofpoint)

As more governments around the world offer stimulus payments and financial assistance to citizens and businesses, the lures have shifted, says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint.

©2018 CliftonLarsonAllen LLP

Example Coronavirus email - March



From: Blanche Wright <contact@asdmark.org>
Sent: Mon 3/30/2020 7:54 AM
To:
Cc:
Subject: Avoid Coronavirus Scams. Read!!!

Dear customer

Avoid Coronavirus Scams
Here are some tips to help you keep the scammers at bay.

Do you want to see which emails are scammers? Scammers send spam emails in a bid to dupe the victims into thinking they can order face masks that will keep them safe from the novel coronavirus. What happens instead is that the victims will unwittingly reveal their sensitive personal and financial information to the fraudsters.

President Coronavirus guidance [asdmark.org]

Kind Regards

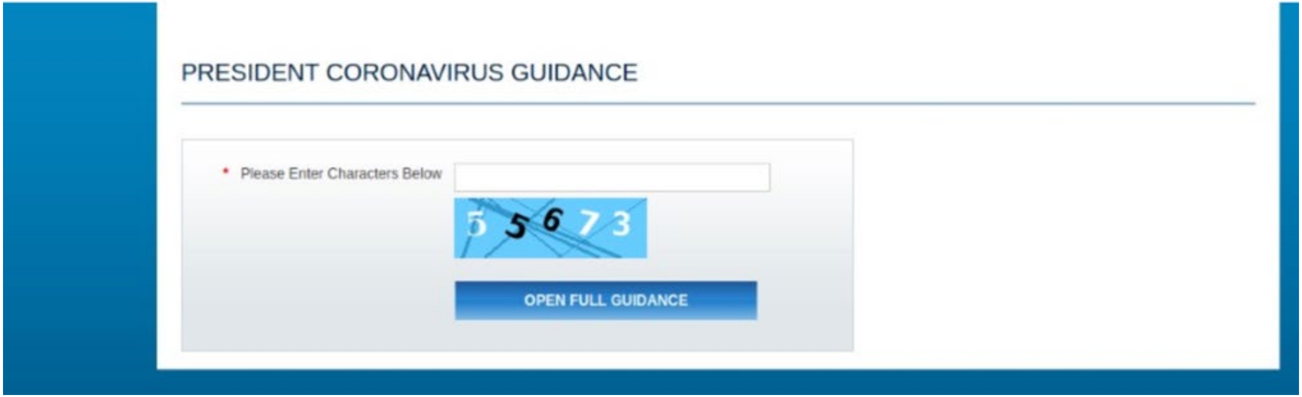
Blanche Wright

- Contains URLs linking to a landing page that presents a CAPTCHA challenge

©2018 CliftonLarsonAllen LLP

CAPTCHA is legit?

©2018 CliftonLarsonAllen LLP



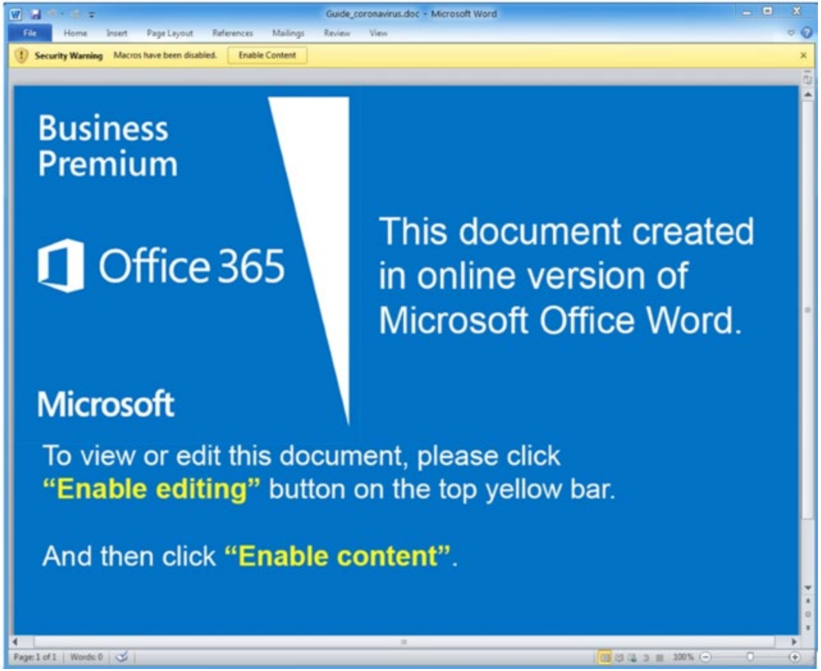
PRESIDENT CORONAVIRUS GUIDANCE

* Please Enter Characters Below

- CAPTCHA challenge launches Word

Never Enable Editing/Enable Content

- The document contained macros that, if enabled, would then download ZLoader version “1.1.21.0.”



Security Warning Macros have been disabled.

Business Premium

Office 365

This document created in online version of Microsoft Office Word.

Microsoft

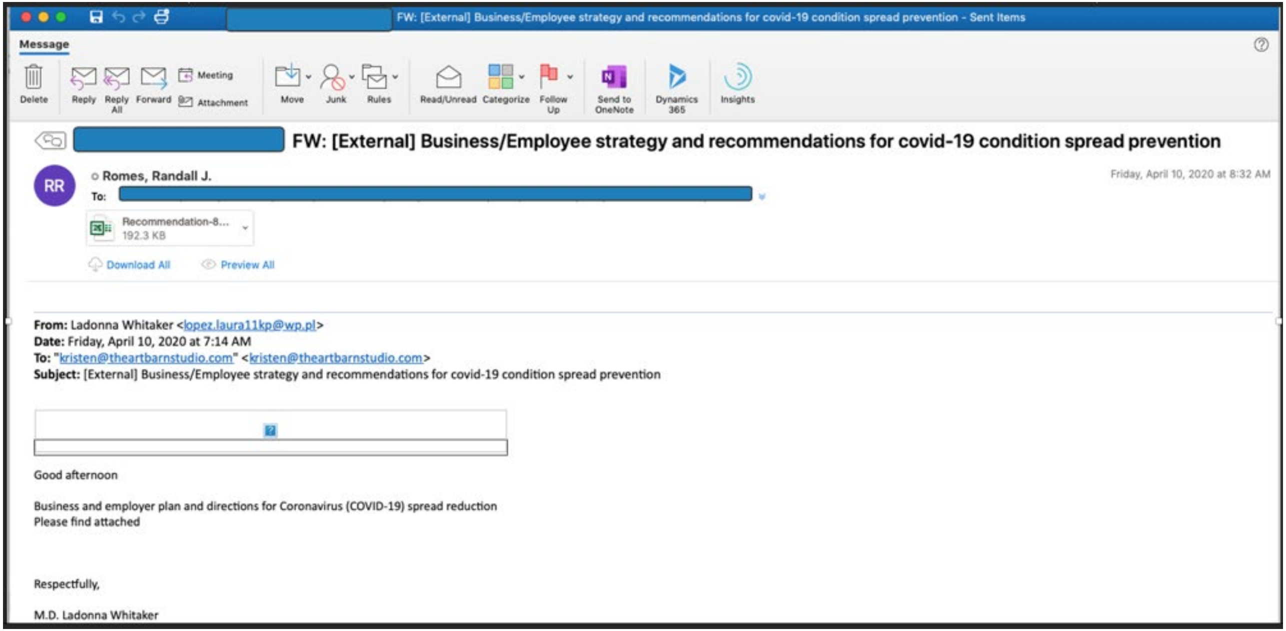
To view or edit this document, please click **“Enable editing”** button on the top yellow bar.

And then click **“Enable content”**.

©2018 CliftonLarsonAllen LLP

COVID Related Phishing

©2018 CliftonLarsonAllen LLP



[redacted] FW: [External] Business/Employee strategy and recommendations for covid-19 condition spread prevention - Sent Items

[redacted] FW: [External] Business/Employee strategy and recommendations for covid-19 condition spread prevention

RR ○ Romes, Randall J.

Friday, April 10, 2020 at 8:32 AM

To: [redacted]

Recommendation-8...
192.3 KB

From: Ladonna Whitaker <lopez.laura11kp@wp.pl>
Date: Friday, April 10, 2020 at 7:14 AM
To: "kristen@theartbarnstudio.com" <kristen@theartbarnstudio.com>
Subject: [External] Business/Employee strategy and recommendations for covid-19 condition spread prevention

Good afternoon

Business and employer plan and directions for Coronavirus (COVID-19) spread reduction
Please find attached

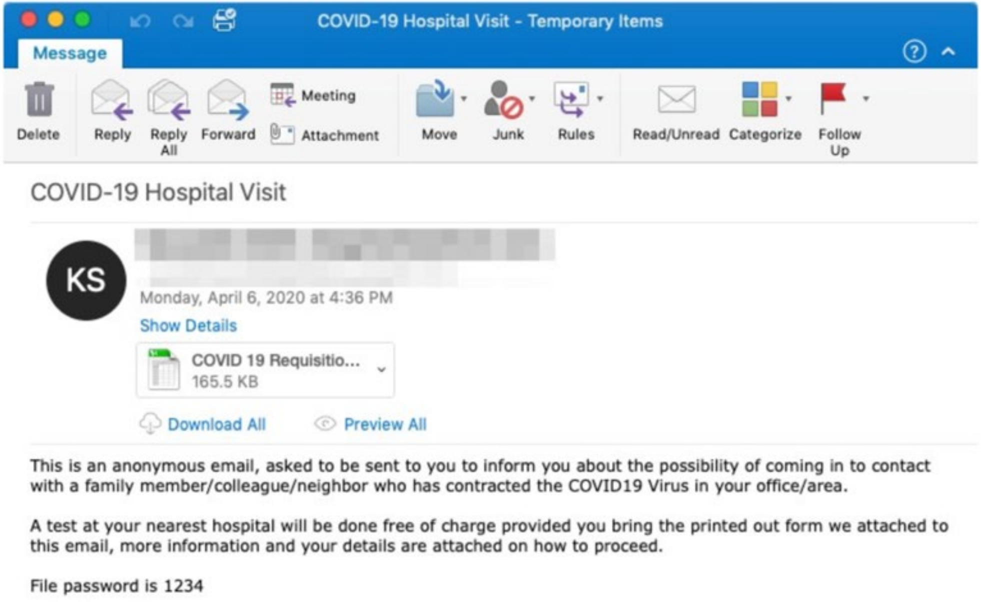
Respectfully,

M.D. Ladonna Whitaker

- Other COVID Scams (BankInfoSecurity . Com):
- **Enhanced Zeus Sphinx Trojan Used in COVID-19 Schemes**
- https://www.bankinfosecurity.com/enhanced-zeus-sphinx-trojan-used-in-covid-19-schemes-a-14267?rf=2020-05-13_ENEWS_SUB_BIS__Slot1_ART14267&mkt_tok=eyJpIjoiWlRrNE1HRmlOMlF4TWpRNCIsInQiOiJ1OThtTGZpOFlsaGNIa2hJVHN0VmxMdlpwWnFCRmJiOWlqMndsUVNLck9mYlZyRXFTMkc3YmZzdTRwbHFsazRuVXhESkNpQ2thWmFneEt5QTU1Ym5cL0R1WFRLYVVPOWlSWkxRYkg3ZjdcL3dkV2FmNUhacEszakVMUlg5V0NydFwvUCJ9a

Example COVID-19 email - April

- Email contains password-protected Excel sheets (Figure 12). The sheet utilized Excel 4.0 macros to download and execute the ZLoader version "1.1.22.0."



COVID-19 Hospital Visit

[redacted]

Monday, April 6, 2020 at 4:36 PM

COVID 19 Requisitio...
165.5 KB

This is an anonymous email, asked to be sent to you to inform you about the possibility of coming in to contact with a family member/colleague/neighbor who has contracted the COVID19 Virus in your office/area.

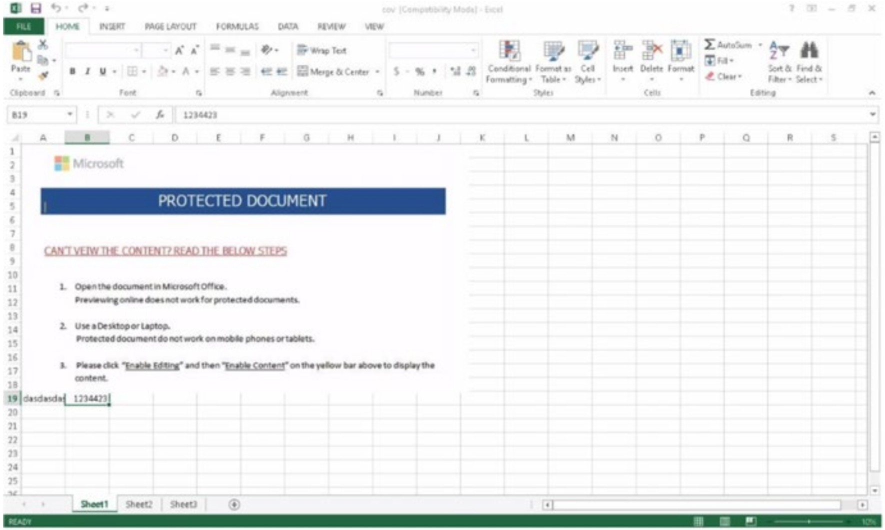
A test at your nearest hospital will be done free of charge provided you bring the printed out form we attached to this email, more information and your details are attached on how to proceed.

File password is 1234

©2018 CliftonLarsonAllen LLP

Macro Enabled

- The spreadsheet contained macros that, if enabled, would then download ZLoader



1234423

Microsoft

PROTECTED DOCUMENT

CAN'T VEIW THE CONTENT? READ THE BELOW STEPS

1. Open the document in Microsoft Office.
   Previewing online does not work for protected documents.

2. Use a Desktop or Laptop.
   Protected document do not work on mobile phones or tablets.

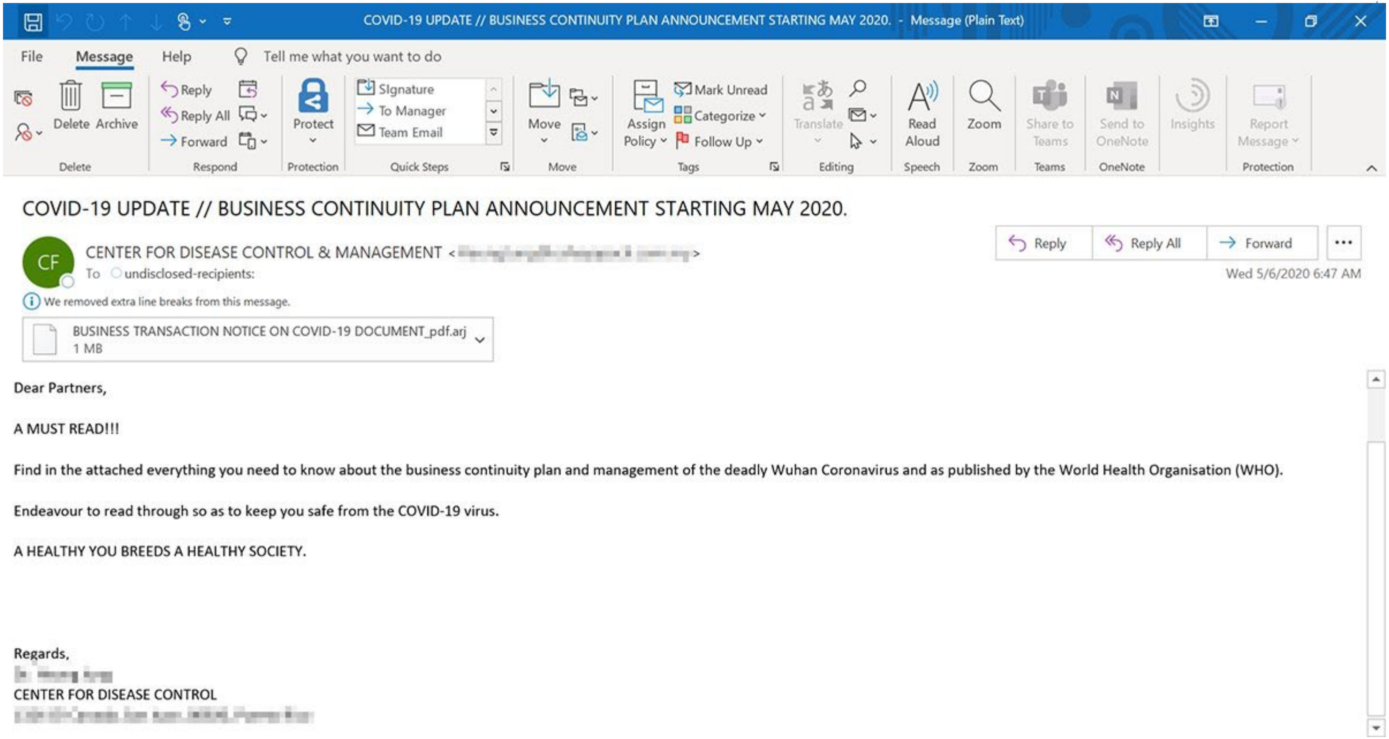
3. Please click "Enable Editing" and then "Enable Content" on the yellow bar above to display the content.

dasdasda 1234423

©2018 CliftonLarsonAllen LLP

COVID Related Phishing

arsonAllen LLP



COVID-19 UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MAY 2020.

CF CENTER FOR DISEASE CONTROL & MANAGEMENT <[redacted]>

To undisclosed-recipients:

Wed 5/6/2020 6:47 AM

We removed extra line breaks from this message.

BUSINESS TRANSACTION NOTICE ON COVID-19 DOCUMENT_pdf.arj
1 MB

Dear Partners,

A MUST READ!!!

Find in the attached everything you need to know about the business continuity plan and management of the deadly Wuhan Coronavirus and as published by the World Health Organisation (WHO).

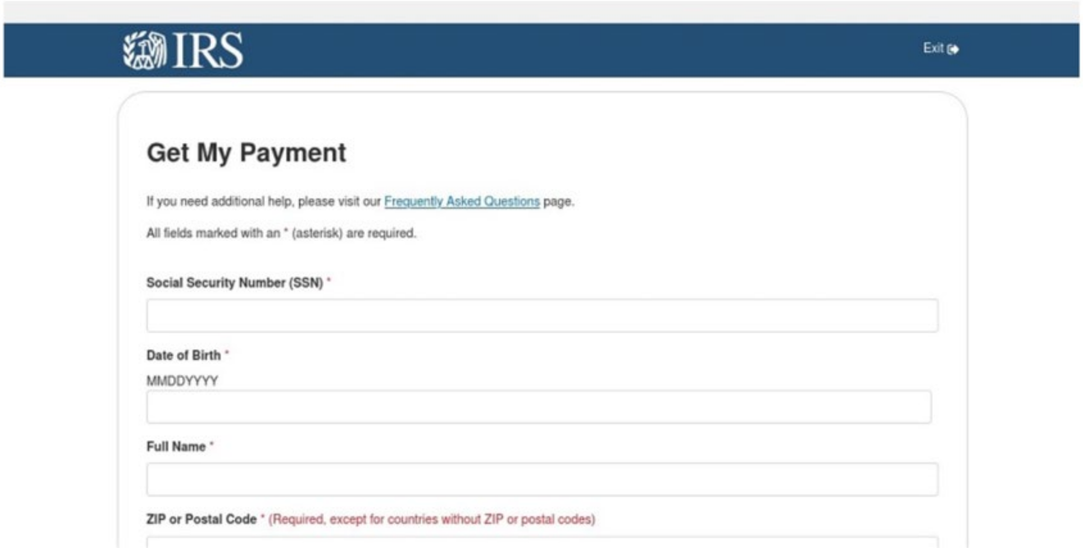
Endeavour to read through so as to keep you safe from the COVID-19 virus.

A HEALTHY YOU BREEDS A HEALTHY SOCIETY.

Regards,
[redacted]
CENTER FOR DISEASE CONTROL
[redacted]

COVID “Opportunities”

A template spoofing the IRS website, which contains multiple pages, displays a fake offer of financial aid as part of a COVID-19 relief program, according to Proofpoint. The site urges victims to click "continue," which then takes them to a form asking for sensitive personal information, including Social Security numbers, full names, dates of birth and postal codes.



Get My Payment

If you need additional help, please visit our Frequently Asked Questions page.

All fields marked with an * (asterisk) are required.

Social Security Number (SSN) *

Date of Birth *

MMDDYYYY

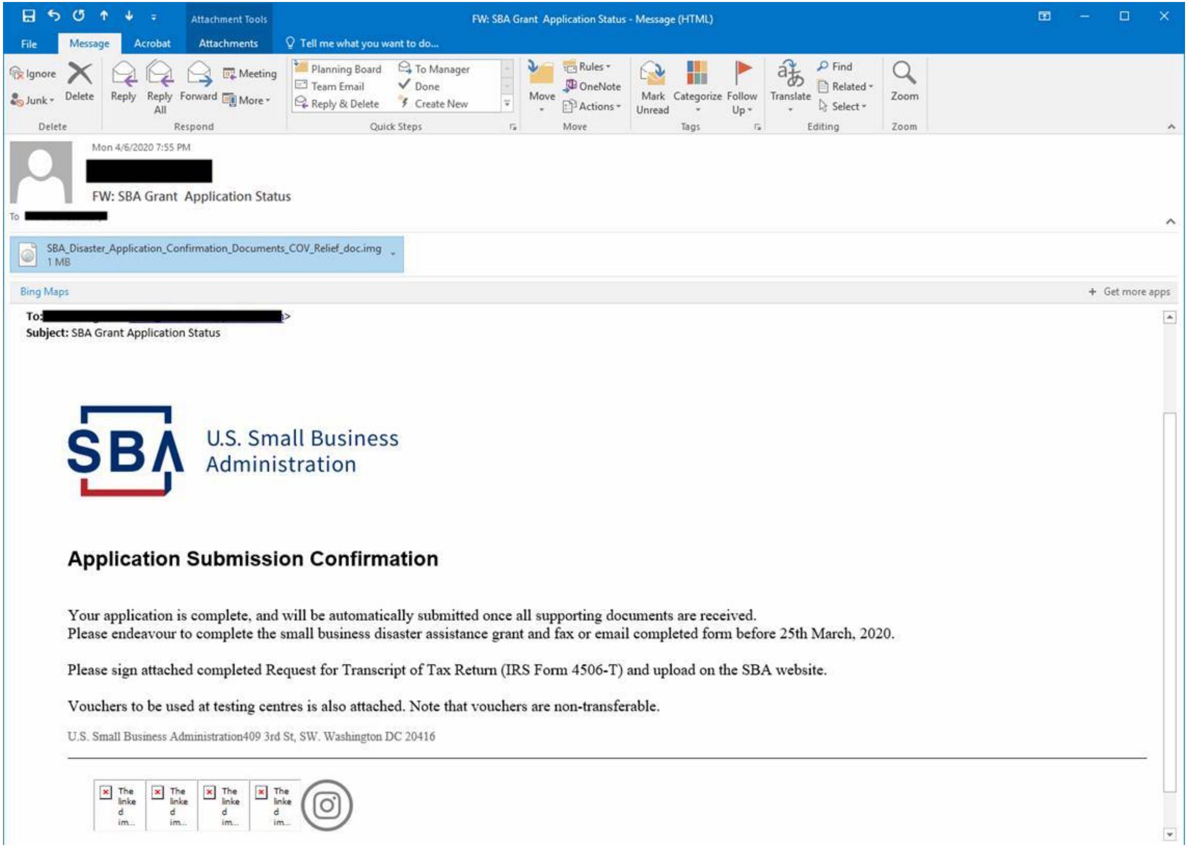
Full Name *

ZIP or Postal Code * (Required, except for countries without ZIP or postal codes)

Fake IRS website template (Source: Proofpoint)

©2018 CliftonLarsonAllen LLP

COVID “Opportunities”



FW: SBA Grant Application Status - Message (HTML)

Mon 4/6/2020 7:55 PM

[redacted]

FW: SBA Grant Application Status

To [redacted]

SBA_Disaster_Application_Confirmation_Documents_COV_Relief_doc.img
1 MB

To:[redacted]>
Subject: SBA Grant Application Status

SBA U.S. Small Business Administration

Application Submission Confirmation

Your application is complete, and will be automatically submitted once all supporting documents are received.
Please endeavour to complete the small business disaster assistance grant and fax or email completed form before 25th March, 2020.

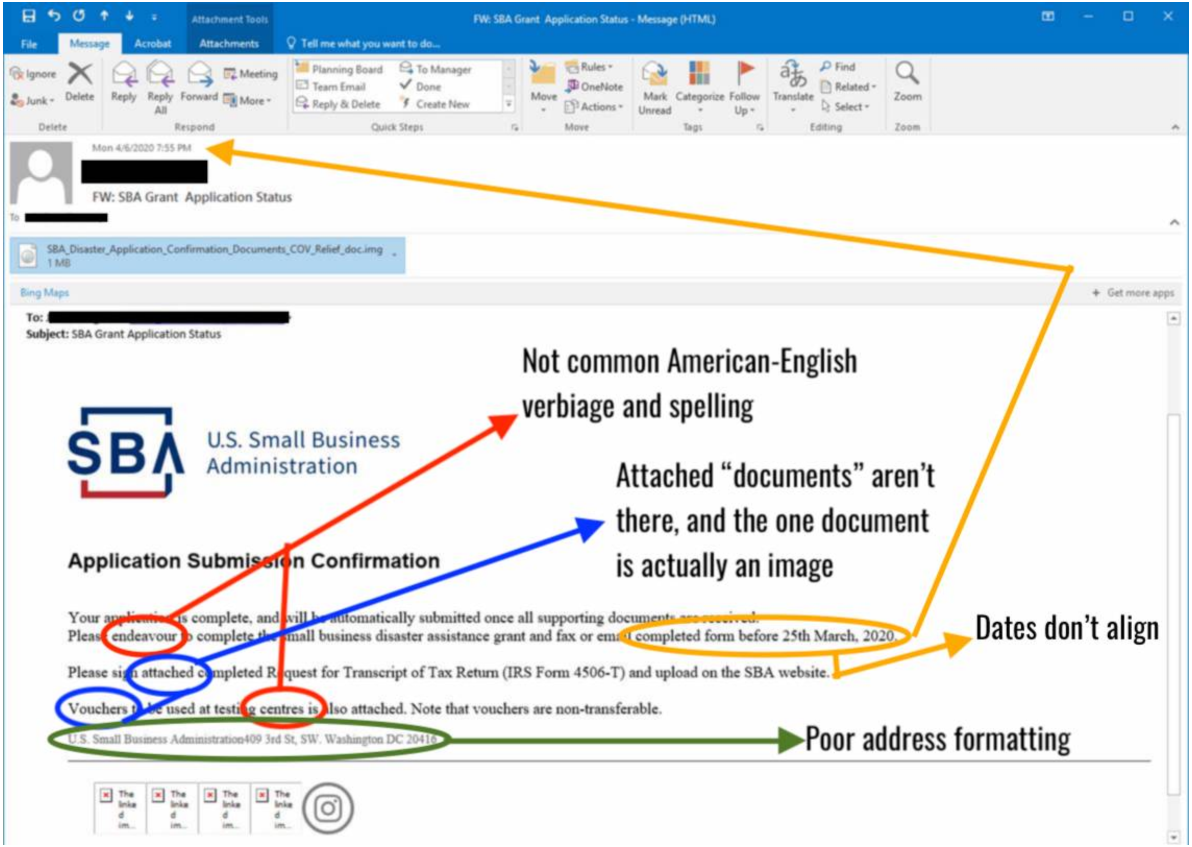
Please sign attached completed Request for Transcript of Tax Return (IRS Form 4506-T) and upload on the SBA website.

Vouchers to be used at testing centres is also attached. Note that vouchers are non-transferable.

U.S. Small Business Administration409 3rd St, SW. Washington DC 20416

©2018 CliftonLarsonAllen LLP

COVID “Opportunities”



Mon 4/6/2020 7:55 PM

[redacted]

FW: SBA Grant Application Status

To [redacted]

SBA_Disaster_Application_Confirmation_Documents_COV_Relief_doc.img
1 MB

To: [redacted]
Subject: SBA Grant Application Status

SBA U.S. Small Business Administration

Application Submission Confirmation

Your application is complete, and will be automatically submitted once all supporting documents are received.
Please endeavour to complete the small business disaster assistance grant and fax or email completed form before 25th March, 2020.

Please sign attached completed Request for Transcript of Tax Return (IRS Form 4506-T) and upload on the SBA website.

Vouchers to be used at testing centres is also attached. Note that vouchers are non-transferable.

U.S. Small Business Administration409 3rd St, SW. Washington DC 20416

Not common American-English verbiage and spelling

Attached “documents” aren’t there, and the one document is actually an image

Dates don’t align

Poor address formatting

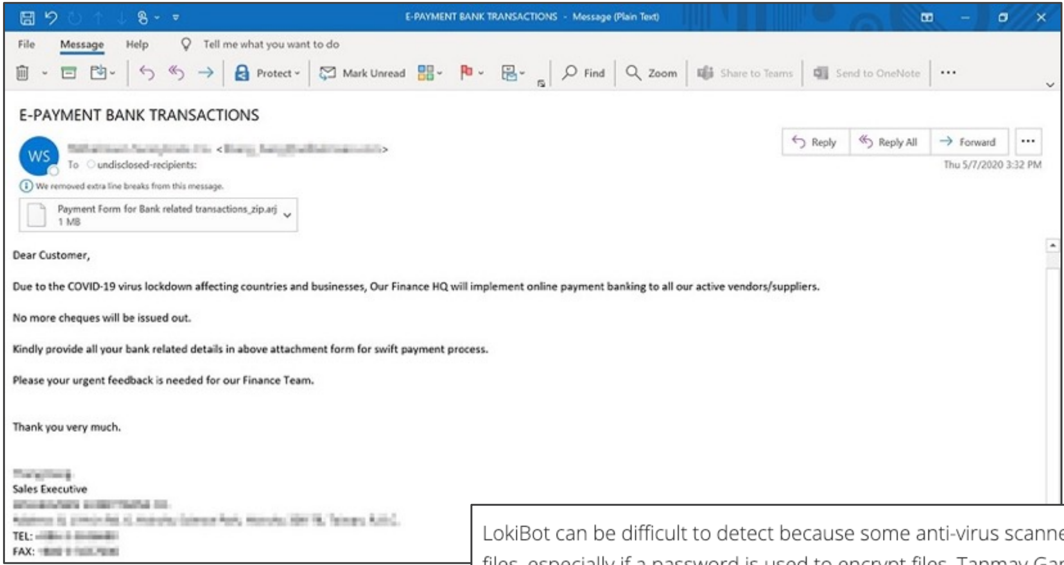
©2018 CliftonLarsonAllen LLP

COVID "Opportunities"

Latest Phishing Emails

Microsoft Security Intelligence first discovered the new phishing tactics in messages dated May 6 and May 7.

The phishing campaigns use ARJ files - a compression format for creating very efficient zipped files. Each file contains a malicious Microsoft Excel file. If it's opened, the LokiBot payload is injected in the Windows' dynamic link library.



E-PAYMENT BANK TRANSACTIONS

[redacted] <[redacted]>
To undisclosed-recipients:

Thu 5/7/2020 3:32 PM

We removed extra line breaks from this message.

Payment Form for Bank related transactions_zip.arj
1 MB

Dear Customer,

Due to the COVID-19 virus lockdown affecting countries and businesses, Our Finance HQ will implement online payment banking to all our active vendors/suppliers.

No more cheques will be issued out.

Kindly provide all your bank related details in above attachment form for swift payment process.

Please your urgent feedback is needed for our Finance Team.

Thank you very much.

[redacted]
Sales Executive
[redacted]
TEL: [redacted]
FAX: [redacted]

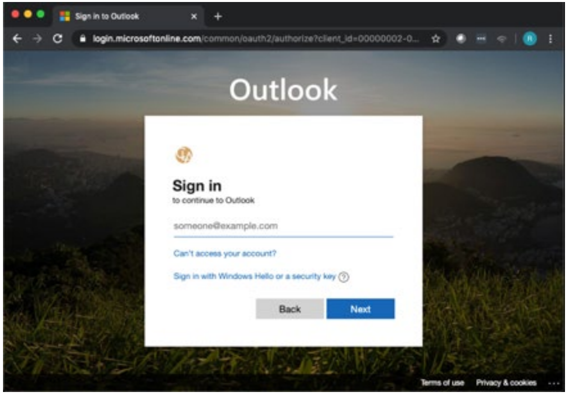
LokiBot can be difficult to detect because some anti-virus scanners will skip checking ARJ files, especially if a password is used to encrypt files, Tanmay Ganacharya, the director of security research at Microsoft Threat Protection, told BleepingComputer.

©2018 CliftonLarsonAllen LLP

COVID “Opportunities”

Attacks on Outlook Web Access

- Password guessing attacks
- Phishing that harvests credentials


Sign in to Outlook

login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0...

Outlook

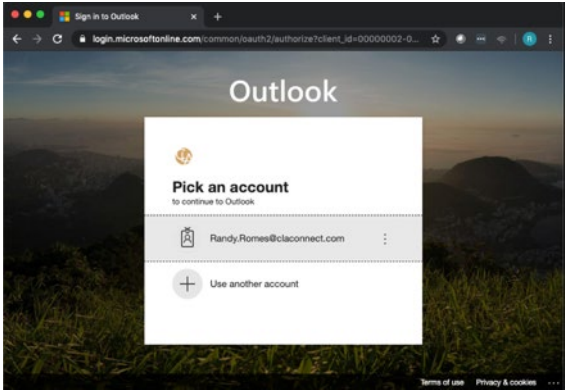
Sign in

to continue to Outlook

someone@example.com

Can't access your account?

Sign in with Windows Hello or a security key


Sign in to Outlook

login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0...

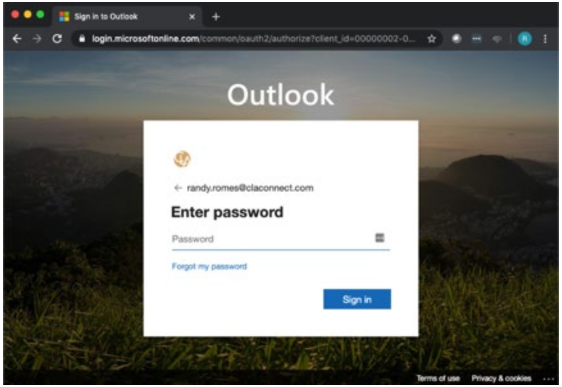
Outlook

Pick an account

to continue to Outlook

Randy.Romes@claconnect.com

Use another account


Sign in to Outlook

login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0...

Outlook

← randy.romes@claconnect.com

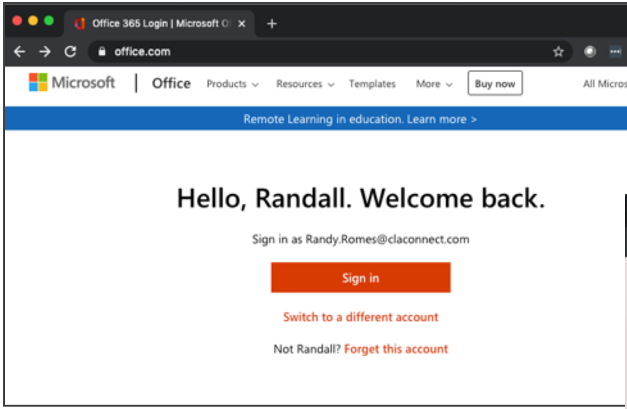
Enter password

Password

Forgot my password

©2018 CliftonLarsonAllen LLP

COVID "Opportunities"



Office 365 Login | Microsoft O

office.com

Remote Learning in education. Learn more >

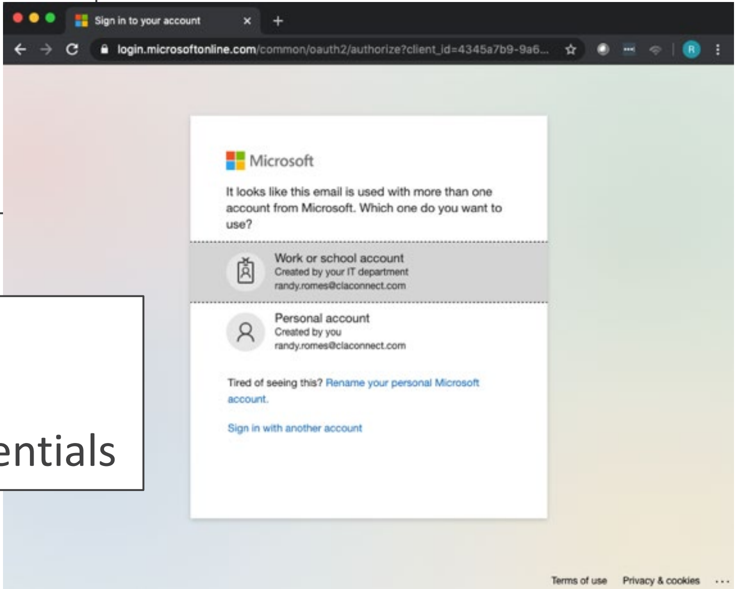
Hello, Randall. Welcome back.

Sign in as Randy.Romes@claconnect.com

Sign in

Switch to a different account

Not Randall? Forget this account



Sign in to your account

login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a6...

Microsoft

It looks like this email is used with more than one account from Microsoft. Which one do you want to use?

Work or school account
Created by your IT department
randy.romes@claconnect.com

Personal account
Created by you
randy.romes@claconnect.com

Tired of seeing this? Rename your personal Microsoft account.

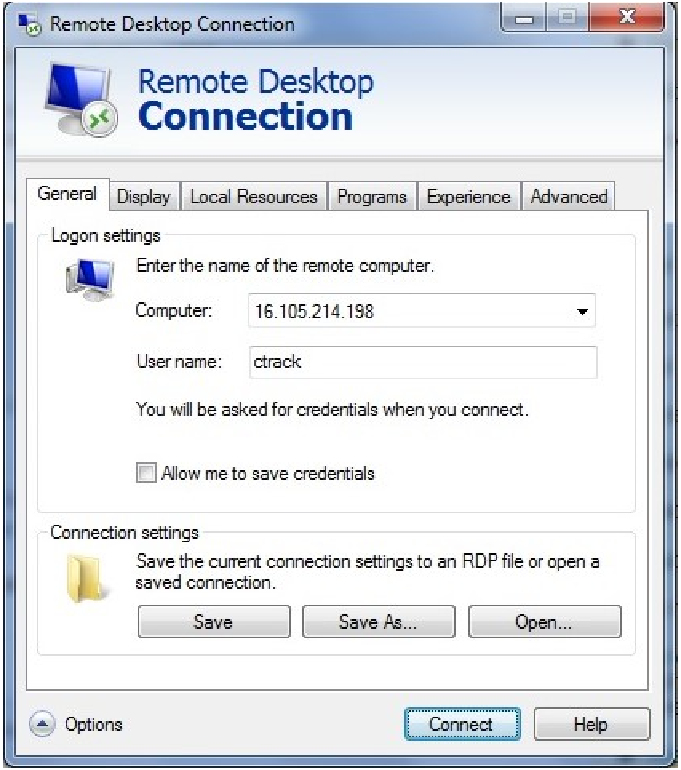
Sign in with another account

Attacks on Office365

- Password guessing attacks
- Phishing that harvests credentials

©2018 CliftonLarsonAllen LLP

COVID "Opportunities"


Remote Desktop Connection

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: 16.105.214.198

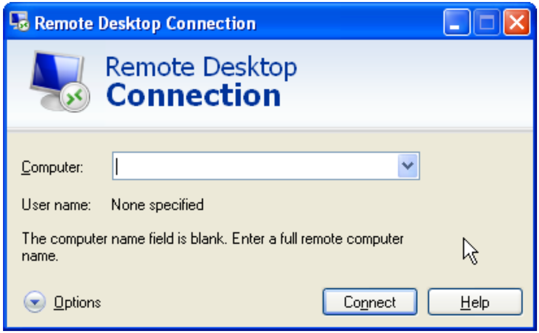
User name: ctrack

You will be asked for credentials when you connect.

☐ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

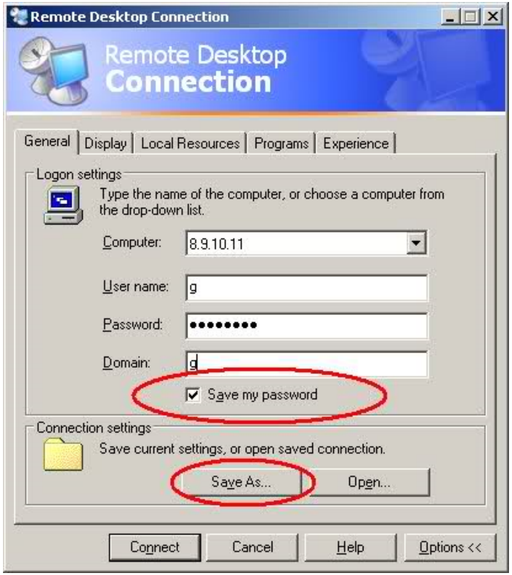

Remote Desktop Connection

Remote Desktop Connection

Computer:

User name: None specified

The computer name field is blank. Enter a full remote computer name.


Remote Desktop Connection

Remote Desktop Connection

Logon settings

Type the name of the computer, or choose a computer from the drop-down list.

Computer: 8.9.10.11

User name: g

Password: ●●●●●●●●●

Domain: g

☑ Save my password

Connection settings

Save current settings, or open saved connection.

©2018 CliftonLarsonAllen LLP

What's Next?

- Security firm Check Point Software discovered nearly 20,000 newly registered domains over the past month are using either COVID-19 or coronavirus as part of their name
- Of these websites, 17% were considered suspicious or malicious, according to the company's report

- Tune your email filters
  - SPF and DMARC
  - "DNS Scoring"

©2018 CliftonLarsonAllen LLP

The Boy Scouts Motto:

“Be Prepared”

Remote Access - How Did Your BCP Fare?

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an
SEC-registered investment advisor

©2018 CliftonLarsonAllen LLP

A Whole New World

We have very quickly gone from “15% remote work force” to instances of “greater than 80% remote work force”.

- What are the “best ways to do this?
- What kind of remote access is acceptable and/or secure?
- What (new) risks do we need to take into consideration?

©2018 CliftonLarsonAllen LLP

Remote Solution Considerations

Accessibility	• Licensing, Open Source, Server Setup
Usability	• Portal, Tunneling, Direct Application
Security	• Encryption, Multi-Factor Authentication, AD integration

©2018 CliftonLarsonAllen LLP

A Wide Variety of Remote Access

1. VPN
   - Traditional clients
   - SSL gateways
2. Remote Desktops
   - In-house applications
3. Application Portals
   - In-house applications
   - Third party systems

➢ Multi-factor authentication (MFA)

©2018 CliftonLarsonAllen LLP

Applications

1. Citrix

2. Office 365
   - Use multi-factor authentication. This is the best mitigation technique to protect against credential theft for O365 administrators and users.
   - Protect Global Admins from compromise and use the principle of "Least Privilege."
   - Enable unified audit logging in the Security and Compliance Center.
   - Enable Alerting capabilities.
   - Integrate with organizational SIEM solutions.
   - Disable legacy email protocols, if not required, or limit their use to specific users.

   https://www.us-cert.gov/ncas/alerts/aa20-120a

➢ Multi-factor Authentication (MFA)

©2018 CliftonLarsonAllen LLP

Planning Remote Access

- **Who** is permitted to connect remotely?
- **What** are they permitted to access?
- **When** are they permitted remote connectivity?
- **Where** are they allowed to connect from?
- **How** are they permitted to connect?

©2018 CliftonLarsonAllen LLP

Securing Your Remote Workforce

©2018 CliftonLarsonAllen LLP

Organization Connectivity

- Ensure the connection is secure (i.e. disallow use of public Wi-Fi)
- Restrict remote access to only those needed timeframes (business hours or current network time restrictions)
- MFA required on any type of access
- Monitoring capability for remote access communications as well as the ability to disable quickly if an issue arises
- Capability to log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, updated IDS and firewall alerts, and follow up on anomalies.
- Strong encryption on all communications (no SSL or TLS prior to 1.2)

The Boy Scouts Motto:

"Be Prepared"

Security of Devices and Home Networks

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

©2018 CliftonLarsonAllen LLP

Securing Your Remote Workforce

Organization-owned Devices

- Company owned devices should be encrypted if they can contain sensitive data
- Application whitelisting on company-owned devices
- Ensure support/functionality for all other in-office security/technology like patch management including antivirus/antimalware updates, vulnerability scanning, event logging/collection, etc

©2018 CliftonLarsonAllen LLP

Securing Your Remote Workforce

Employee-owned Devices

- Anti-malware protection (company provided or use device posture assessment)
- Enforce OS, application, utility & library patching (company provided or use device posture assessment) e.g. Mac OS, MS Office, Adobe Reader, Java Runtime.
- Mobile device management or posture-checking access gateway
- Some assurance that all other devices connecting to the network (i.e. personal devices) meet security and configuration requirements
- Employee owned devices should be restricted from storing company data
- Employee owned devices should be encrypted to protect sensitive information regarding access to the company network

©2018 CliftonLarsonAllen LLP

Home Networks and Remote workforce

- Monitoring, Data Loss Prevention, and Alerting
  - ◊ Your “internal network” may now have end points in your employees basement/bedroom/home office
  - ◊ Where possible you need visibility…
- Help desk/service desk challenges with remote work force
- What else is ”out there”

©2018 CliftonLarsonAllen LLP

The Boy Scouts Motto:

“Be Prepared”

Operational Continuity in a Remote / Virtual Mode

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

©2018 CliftonLarsonAllen LLP

Collaboration Software

Remote Desktop Connection

Microsoft Remote Desktop Connection for Mac

Computer:

(Examples: MyPC, name.microsoft.com, 192.168.2.8)

1. Enterprise
2. Free

GoToMyPC

Wherever you go, GoToMyPC goes.

Connect to work from anywhere on your smartphone or tablet.

Go mobile with GoToMyPC →

- They all do largely the same/similar things
- They all have pros and cons
- They all have software vulnerabilities

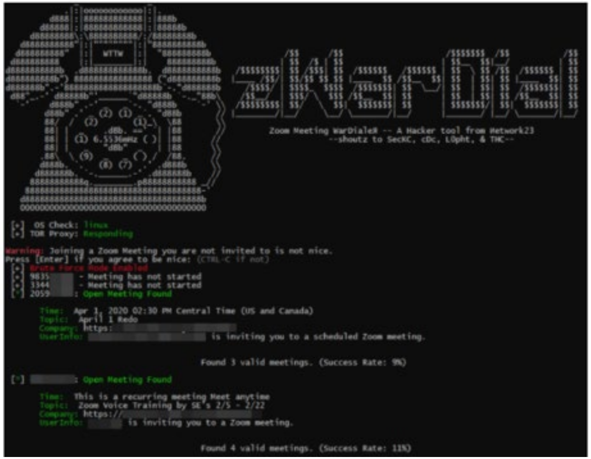
➢ Example…

©2018 CliftonLarsonAllen LLP

Zoom Collaboration Software

Three main issues:

1. "Zoombombing"
2. Hacking exploitable vulnerabilities
3. Questions about encryption



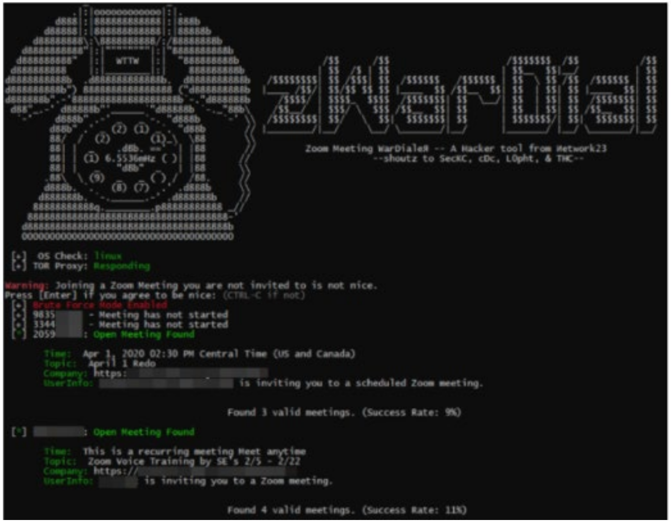
```
                    Zoom Meeting WarDialeR -- A Hacker tool from Network23
                          --shoutz to SecKC, cDc, L0pht, & THC--

 [+]  OS Check: linux
 [+] TOR Proxy: Responding

Warning: Joining a Zoom Meeting you are not invited to is not nice.
Press [Enter] if you agree to be nice: (CTRL-C if not)
 [+] Brute Force Mode Enabled
 [+] 9835[redacted] - Meeting has not started
 [+] 3344[redacted] - Meeting has not started
 [*] 2059[redacted]: Open Meeting Found

      Time:  Apr 1, 2020 02:30 PM Central Time (US and Canada)
      Topic:  April 1 Redo
      Company: https:[redacted]
      UserInfo: [redacted] is inviting you to a scheduled Zoom meeting.

                                        Found 3 valid meetings. (Success Rate: 9%)

 [*] [redacted]: Open Meeting Found

      Time:  This is a recurring meeting Meet anytime
      Topic:  Zoom Voice Training by SE's 2/5 - 2/22
      Company: https://[redacted]
      UserInfo: [redacted] is inviting you to a Zoom meeting.

                                        Found 4 valid meetings. (Success Rate: 11%)
```

©2018 CliftonLarsonAllen LLP

Zoom Collaboration Software

1. “Zoombombing”
   - “Old is new again:” WarDialing
   - Ability to programmatically guess/find meeting IDs
   - 14% success rate

➢ **Easy to prevent**



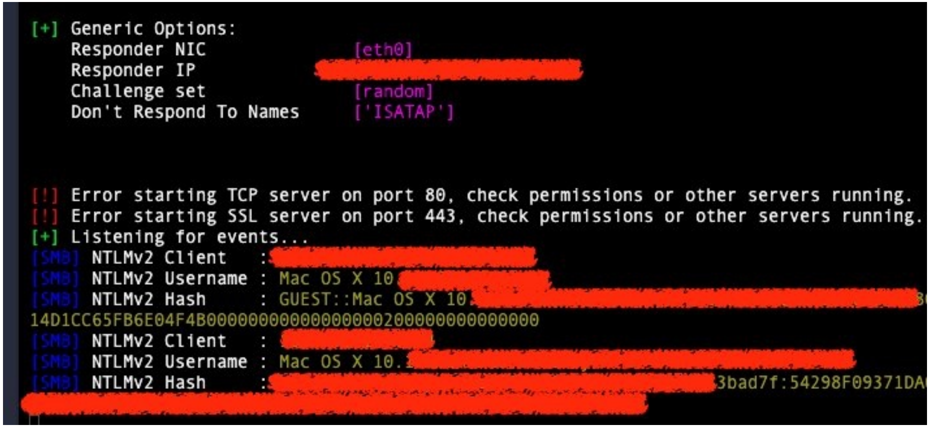
```
Zoom Meeting WarDialeR -- A Hacker tool from Network23
        --shoutz to SecKC, cDc, L0pht, & THC--

[+]  OS Check: linux
[+] TOR Proxy: Responding

Warning: Joining a Zoom Meeting you are not invited to is not nice.
Press [Enter] if you agree to be nice: (CTRL-C if not)
 [+] Brute Force Mode Enabled
 [+] 9835[redacted] - Meeting has not started
 [+] 3344[redacted] - Meeting has not started
 [*] 2059[redacted]: Open Meeting Found

      Time:   Apr 1, 2020 02:30 PM Central Time (US and Canada)
      Topic:   April 1 Redo
      Company: https:[redacted]
      UserInfo: [redacted] is inviting you to a scheduled Zoom meeting.

                          Found 3 valid meetings. (Success Rate: 9%)

 [*] [redacted]: Open Meeting Found

      Time:   This is a recurring meeting Meet anytime
      Topic:   Zoom Voice Training by SE's 2/5 - 2/22
      Company: https://[redacted]
      UserInfo: [redacted] is inviting you to a Zoom meeting.

                          Found 4 valid meetings. (Success Rate: 11%)
```

©2018 CliftonLarsonAllen LLP

Zoom Collaboration Software

2. Hacking exploitable vulnerabilities
   - “Local exploits” allow privilege escalation
   - This means they must already be on/in control of PC

➢ **ie. the PC has already been hacked**

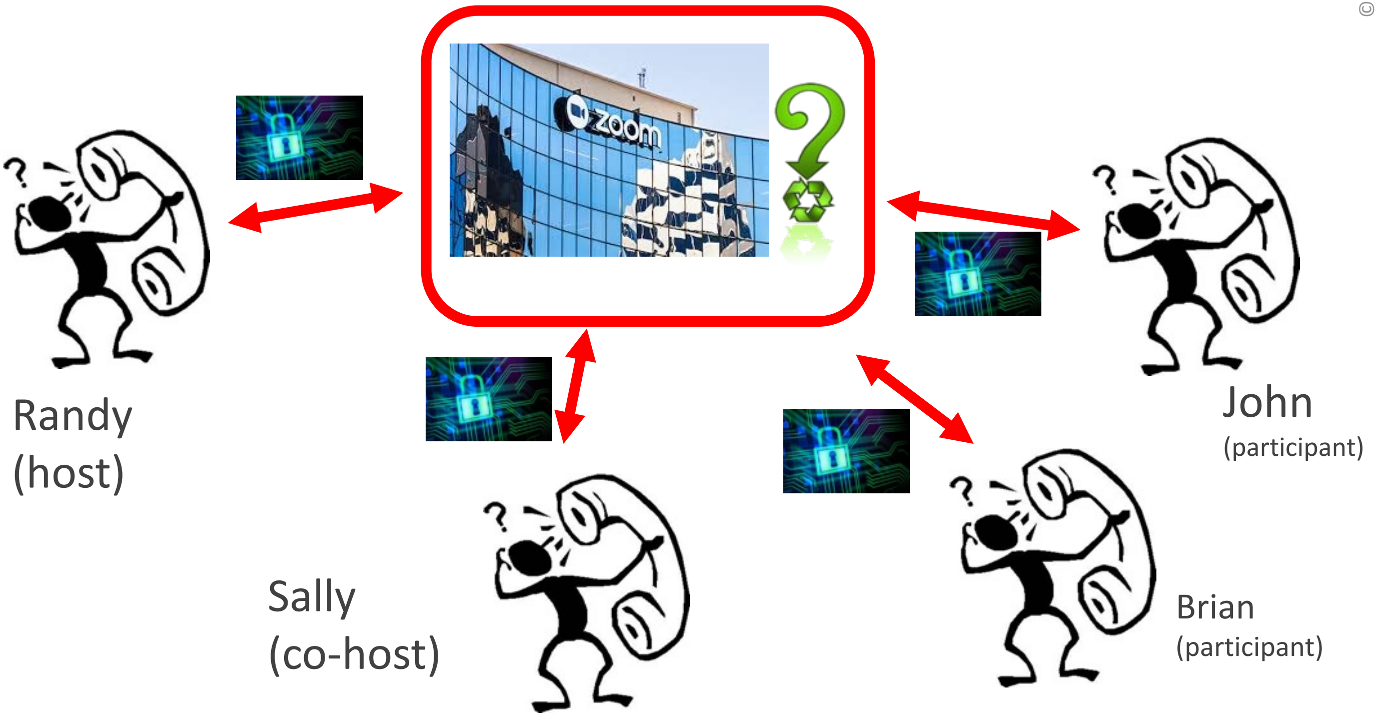


```
[+] Generic Options:
    Responder NIC             [eth0]
    Responder IP              [redacted]
    Challenge set             [random]
    Don't Respond To Names    ['ISATAP']


[!] Error starting TCP server on port 80, check permissions or other servers running.
[!] Error starting SSL server on port 443, check permissions or other servers running.
[+] Listening for events...
[SMB] NTLMv2 Client   : [redacted]
[SMB] NTLMv2 Username : Mac OS X 10[redacted]
[SMB] NTLMv2 Hash     : GUEST::Mac OS X 10[redacted]
14D1CC65FB6E04F4B00000000000000000200000000000000
[SMB] NTLMv2 Client   : [redacted]
[SMB] NTLMv2 Username : Mac OS X 10.[redacted]
[SMB] NTLMv2 Hash     : [redacted]3bad7f:54298F09371DA
[redacted]
```

©2018 CliftonLarsonAllen LLP

Zoom Collaboration Software

3. Questions about encryption?



Randy
(host)

John
(participant)

Sally
(co-host)

Brian
(participant)

©2018 CliftonLarsonAllen LLP

Zoom Collaboration Software

Secure use of Zoom

1. Don’t use personal meeting ID
2. Password protect the meeting(s)
3. Don’t post meeting ID or PW on social media
4. Host/co-host allows participants in
5. Keep your software up to date

https://support.zoom.us/hc/en-us/articles/360033331271-Account-Setting-Update-Password-Default-for-Meeting-and-Webinar

©2018 CliftonLarsonAllen LLP

The Boy Scouts Motto:

"Be Prepared"

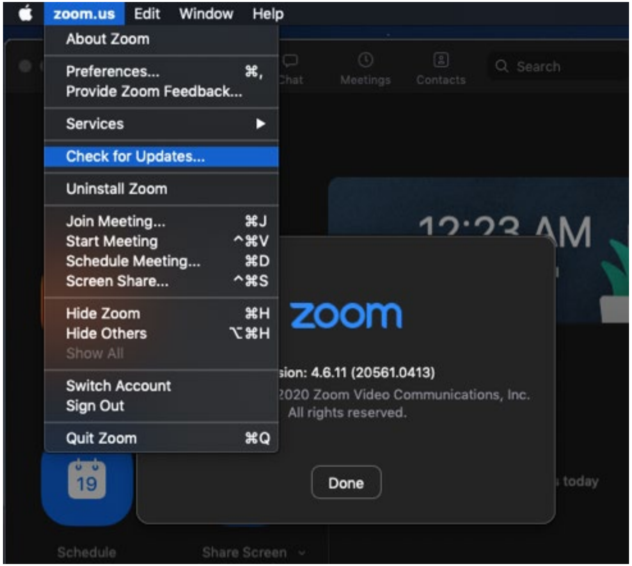
Basic Cyber Hygiene

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

©2018 CliftonLarsonAllen LLP

Personal Cybersecurity Hygiene

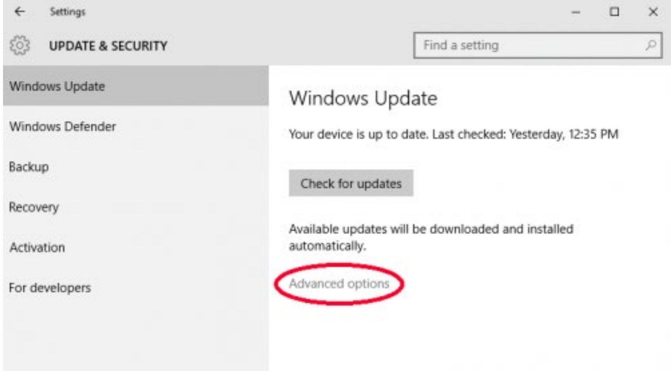
1. Turn on Automatic Updates
2. Manually update your software if necessary
3. Use up to date Antivirus software
4. Choose/use good passwords
5. Email and browsing awareness



©2018 CliftonLarsonAllen LLP

Where to find Automatic Updates

1. Windows 10



Settings

UPDATE & SECURITY

Find a setting

Windows Update

Windows Defender

Backup

Recovery

Activation

For developers

Windows Update

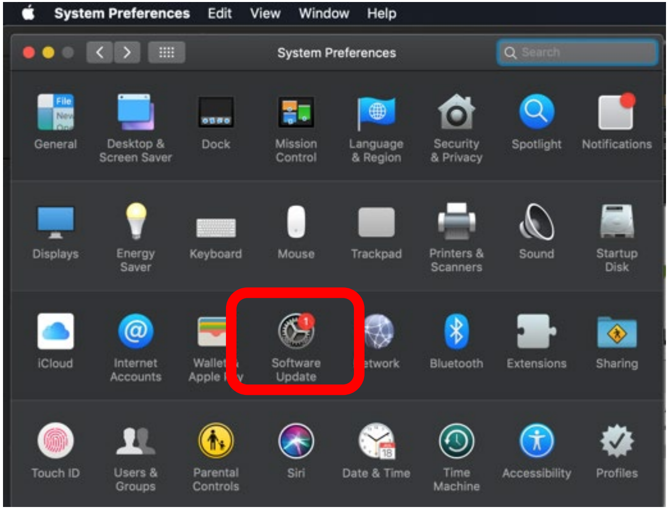
Your device is up to date. Last checked: Yesterday, 12:35 PM

Check for updates

Available updates will be downloaded and installed automatically.

Advanced options

2. Mac OS



©2018 CliftonLarsonAllen LLP

Choosing and Remembering Passwords

- Multi-factor authentication on external systems
- **Pass Phrases – Looooooong natural language**

  Password19 <------------- ***Unforgiveable!***

  Summer19 <------------- *Terrible*

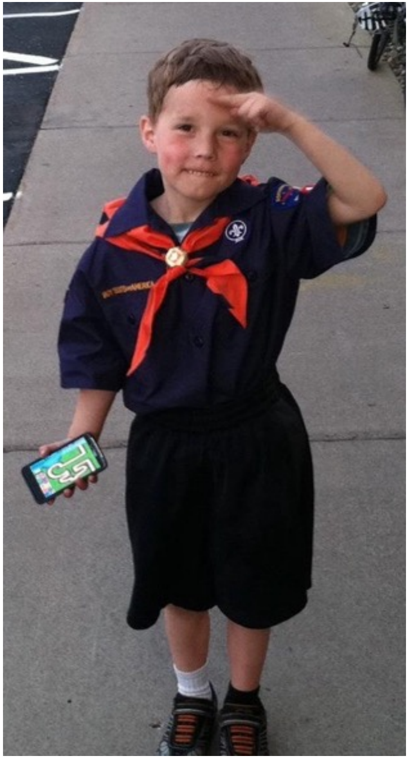
  *N*78fm/1* <------------- *Painful*

  Wallet Painting lamp <-- GOOD

  The Badgers win virtual ESPN bracket! <-- BEST

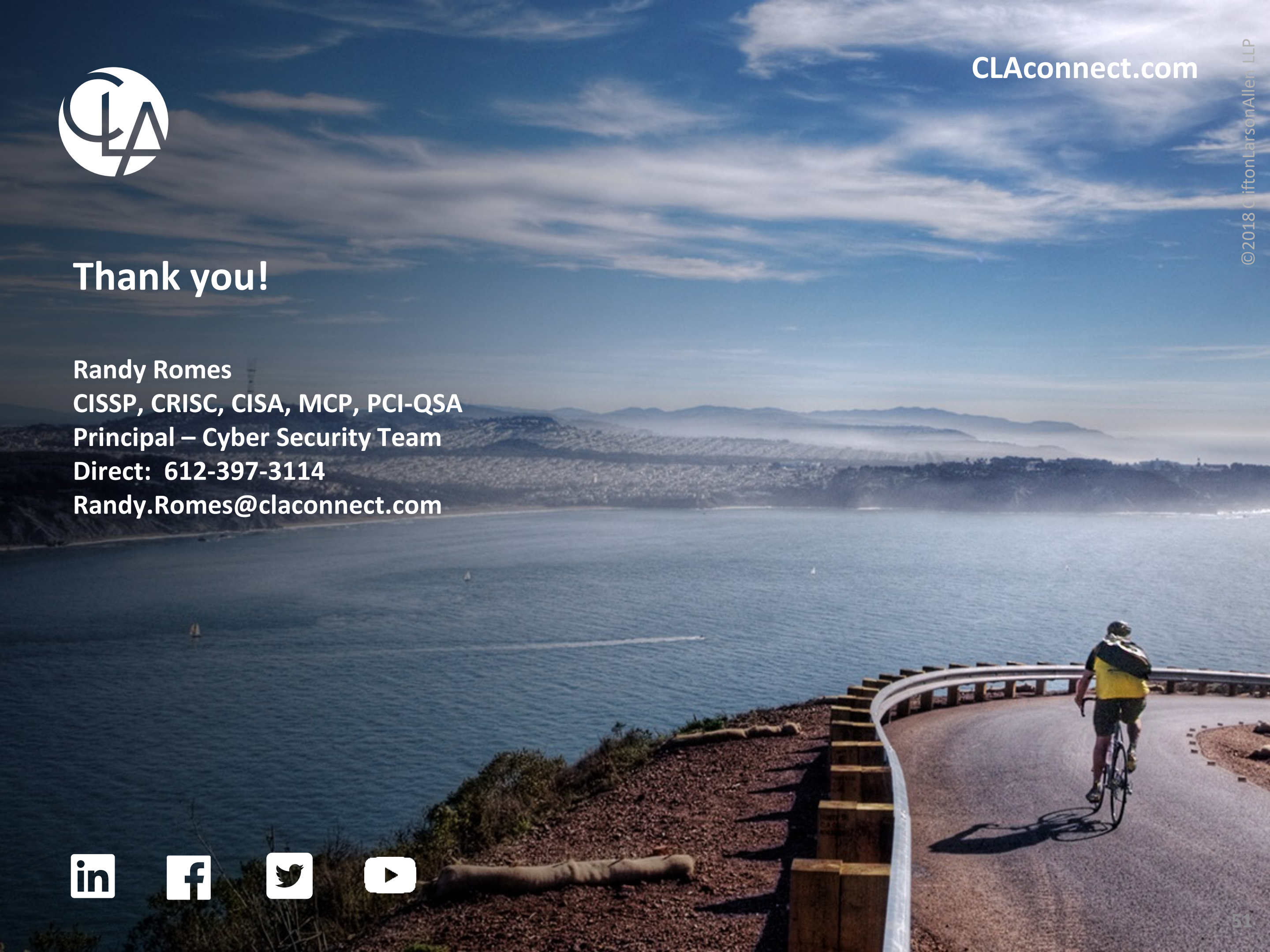
- Password managers (LastPass, 1Password…)

©2018 CliftonLarsonAllen LLP



Questions?

©2018 CliftonLarsonAllen LLP



CLAconnect.com

Thank you!

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA
Principal – Cyber Security Team
Direct: 612-397-3114
Randy.Romes@claconnect.com

©2018 CliftonLarsonAllen LLP