XTERRALINK

Public Sector, Private and Healthcare Divisions

Security Hygiene Education Brief

The **VERY FEW** Steps to protect YOUSELF at home against COMPUTER HACKERS!!!

903 Fulton Ave. Suite 408
Sacramento, CA 95825
https://www.xterralink.com/contact-us

CMAS: 3-12-70-2916a

(888) 444-9995

SB Micro: #1739057

"White Shark Kayak 140 MB Scan b-®Thomas P. Peschak.jpg"

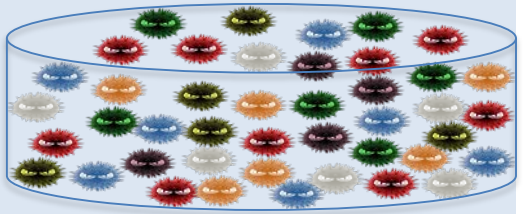
Outline for today

- Believe
- Command and Control – with Your COMPUTER as one of the nodes
- It Really Happens – Scenarios
- Preventable Measures

Believe

Cont'd

- *Your computer is performing sluggish, you get a popup telling you that your computer has …*



- *You drive into your home parking to realize that your home has been vandalized and your computer with lots of sensitive passwords is stolen?*

- *Your wife tells you they just sent an email with sensitive personal attachment to one of your friends accidently?*

Believe

Cont'd

- *You receive a call letting you know that your car was stolen; you had a hard disk in the car and a laptop with client information?*
- *You are checking into the airline, and you decided to check-in your laptop?*
- *You arrive at a restaurant, and decide to put your laptop in the trunk; someone is watching you?*

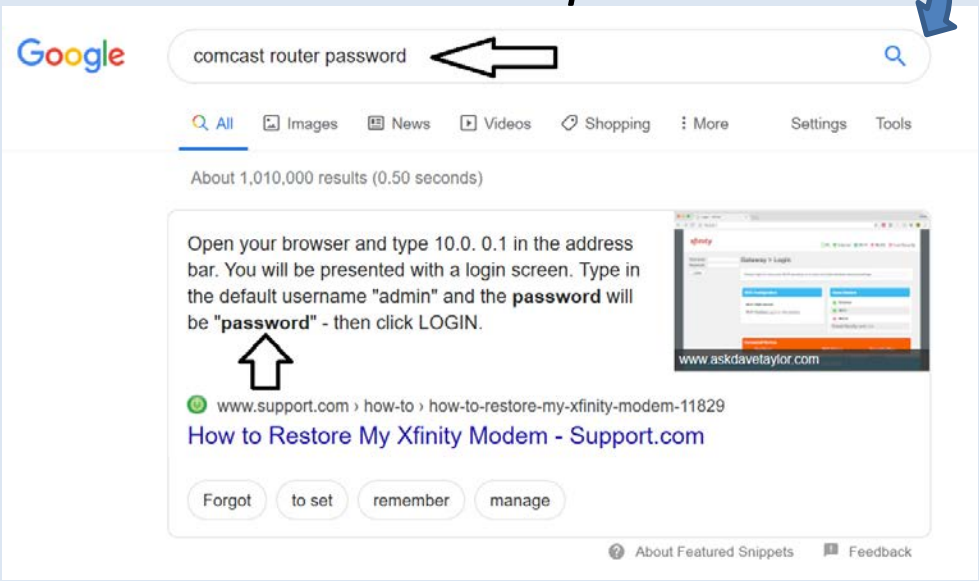
You Don't think this happens, it really happened and more…

Believe

Cont'd

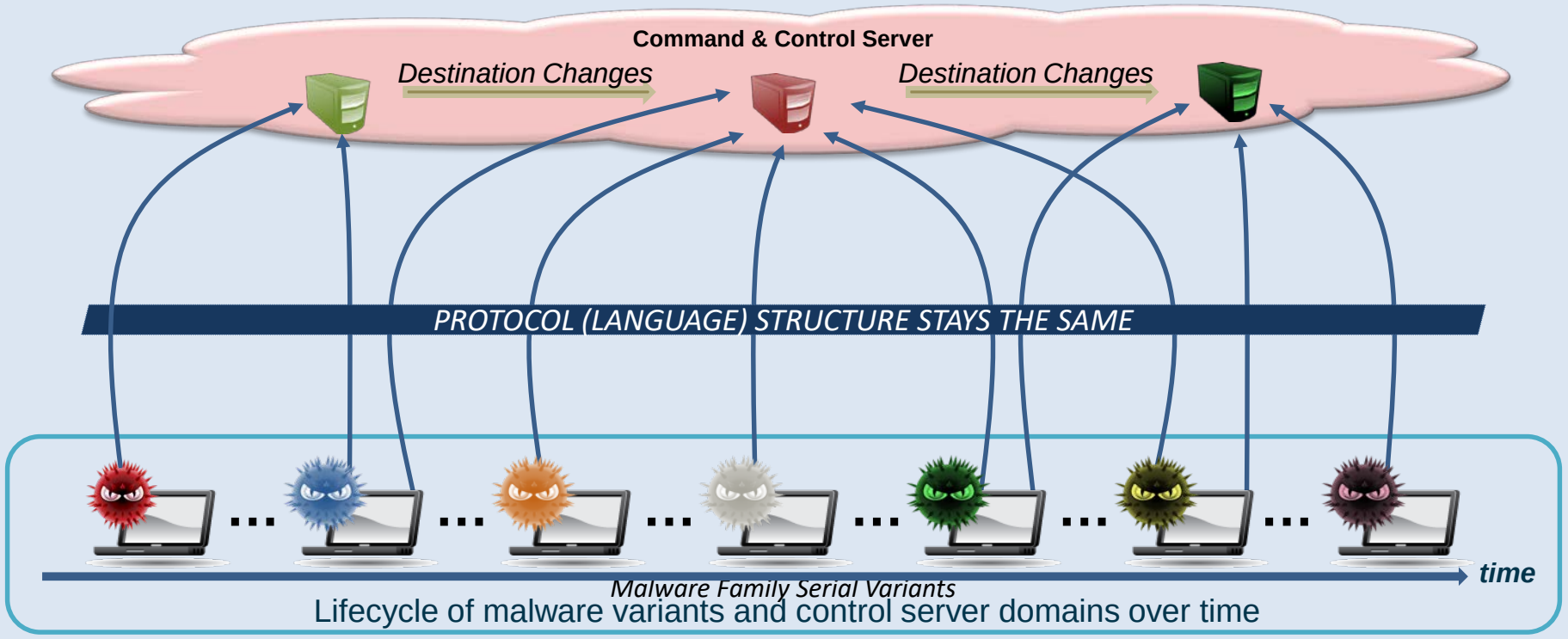
1. 12345
2. 123456
3. 123456789
4. test1
5. password
6. 12345678
7. zinch
8. g_czechout
9. asdf
10. qwerty
11. 1234567890
12. 1234567
13. Aa123456.
14. iloveyou
15. 1234
16. abc123
17. 111111
18. 123123
19. dubsmash
20. test

- *You can search a Cable router password?*



- *Top 10 used Passwords in 2019 are …*

Command and Control – With YOUR COMPUTER as one of the nodes



Lifecycle of malware variants and control server domains over time

The evolution of a malware… from a simple ad-ware to a complex virus that steels info.

Stuff of Science Fiction?
Independence day movie you say. Huh…

Source: Damballa

It Really Happens – Scenarios

The next set of scernarios way scammers / hackers will try to trick YOU; be careful!!

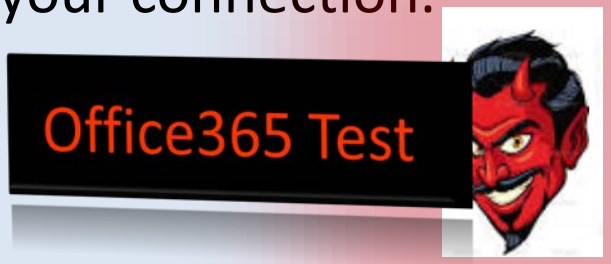
It Really Happens – Scenarios

What would you do if …

Email Subject: Your Outlook® Connection issues

Email Body: We are trying to reach you because your Microsoft account has been unstable, and we need to test your connection. Please press the link below to log on to your account to test your connection.

Sincerely,
Office365 Team,
Microsoft Support.



This email seems to be legitimate, directed from Microsoft Outlook® Team?

It Really Happens – Scenarios

What would you do if …

Email Subject: Your Bank Account is Locked

Email Body: We noticed suspicious activities on your account and we need to validate your account information. Please use the link below to logon to your account.

Sincerely,
Bank of America,
Online Support.

This email seems to be legitimate, directed from BofA Team?

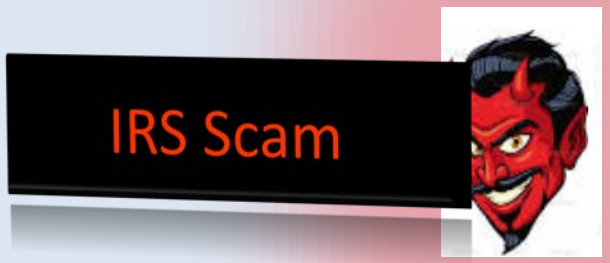
It Really Happens – Scenarios

What would you do if …

Email Subject: IRS Payment Delinquent

Email Body: This the IRS, and you have payments that are past due. Please call the number below to resolve the debt. You will be able to pay online through the online payment process.

Sincerely,
Internal Revenue Service.



This email seems to be legitimate, directed from the IRS?

It Really Happens – Scenarios

Cont'd

What would you do if …

Email Subject: Will, Pay for driving on toll road, invoice #0000645095

Email Body: Dear Will, You have a debt to pay for using a toll road. Please service your debt in the shortest possible time. The copy of the invoice is attached to this email.

Sincerely,
Mark Mann,
E-ZPass Support.

This email seems to be legitimate, directed from your FastTrack Maybe?
But your legal name is really William? hmmmmm

It Really Happens – Scenarios

Cont'd

What would you do if …

Email Subject: Dr. John Smith sent you important documents

Email Body: Dr. John Smith used Google drive to share your xRays with you securely. Click the link and logon and view the xRays.

Sincerely,
Dr. John Smith,
EZDental.

This email seems to be legitimate, directed from Dr. John Smith?

It Really Happens – Scenarios

Cont'd

What would you do if …

Computer: Your Computer Displays Popups

Pop Up: Your Computer is at risk, there are viruses that are causing your computer to run slow. Press the Link below to see a report and contact our Microsoft Support.

This Pop Ups are nothing but a fake script. Press <Esc> and Reboot PC.

It Really Happens – Scenarios

Cont'd

What would you do if …

Computer: Singles In Your Area Popups

Pop Up: View singles in your area, press the link.

This will install more pop ups and possibly viruses; websites are untrusted.

It Really Happens – Scenarios

Cont'd

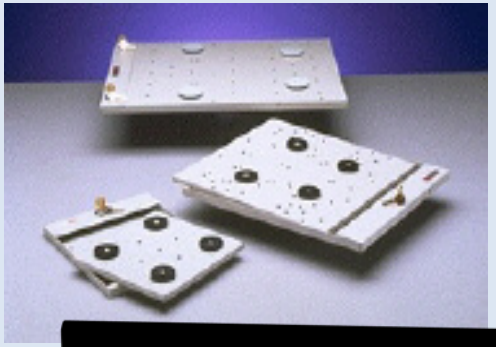
What would you do if …

Software Installation: You Install Software

Free Software: You install software and press "Next", then "Next" then "Finish"… Before you know it, you've installed additional pieces of Software without knowing it.

Read before you press Next… Uncheck boxes to install more than what you need.

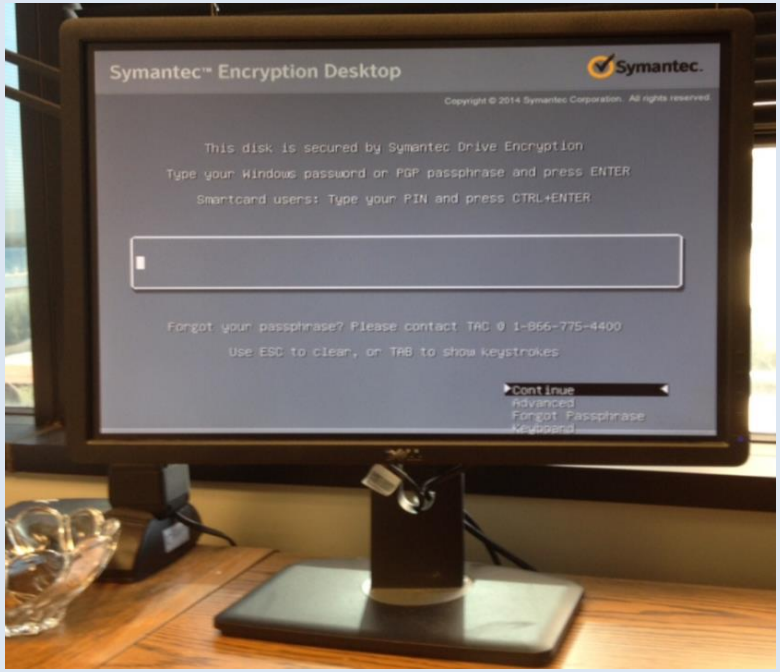
Preventable Measures

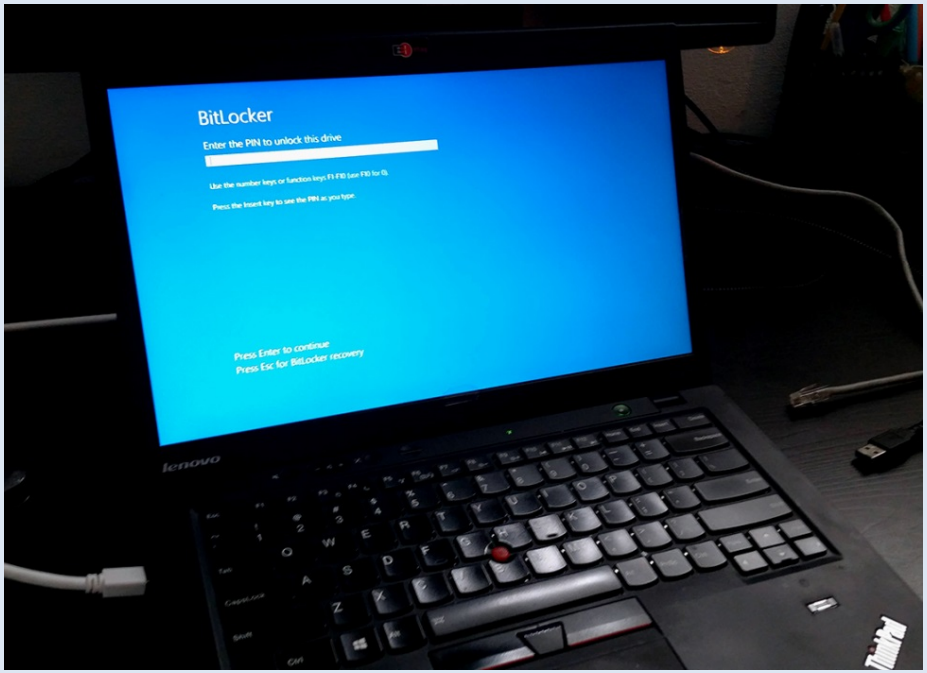


Lock it down or lock it up…

Preventable Measures

Cont'd





Encrypt it before it leaves your computer …

Preventable Measures

Cont'd

Shop for encrypted usb drive on Google

Sponsored ⓘ

Kingston DataTraveler...
$26.99
CDW

Sandisk - Connect 32gb...
$59.99
Best Buy

IronKey Enterprise D2...
$109.99
CDW

Aegis Secure Key 3.0 240G...
$369.00
Apricorn

CORSAIR Padlock 2 16...
$35.99
Newegg B...

Encrypt it before it leaves you … Use BitLocker for thumb Drives or purchase protected drives.

Preventable Measures

Cont'd

Use Case	Recommendation
Personal vs. Professional Use	• Avoid mixing personal and profession use • Download ONLY reputable software
Malware Protection	• Purchase reputable anti-virus • Purchase reputable anti-malware • Turn signature updates and real-time protection on
Patching	• Subscribe to on-line patching services • Follow operating system updates
Bluetooth	• Turn off Bluetooth and automatic pairing
Wireless & Routers	• Turn on strong router security • Change the administrative password • Turn off SSID broadcast feature (optional)
Mobile Text Message	• Some text messages will redirect you automatically to open your mobile browser. Android is vulnerable and may download viruses onto your phone
Back up YOUR Computer	• Purchase a USB or an external device and BACKUP your computer ALWAYS!!! • Ransomware only affect immediately connected devices ONLY (e.g., you download Ransomware while you are backing up) – be careful!!!

Preventable Measures

Cont'd

Use Case	Recommendation
Passwords	• Change default passwords • Use complex passwords • Change your passwords frequently • Use different passwords or use a **Password Manager** • Use passwords as passphrase " !LoveBa$eB@ll" • If you must, use the same password but different letters • Don't sign on as an administrator to your computer, create a limited access account
Firewalls	• Turn firewall protection on
Email Protection	• Don't open emails from unknown senders • Don't open the link from the email • Don't open attachments within emails • **Copy**, and then paste the link into the browser, do NOT press the link with the email • Hover over and see details of the link in your browser • However with the mouse and the cursor over email address to see the sender full email if you know them
Social Media	• Do NOT just befriend anyone • Do NOT advertise your plans (e.g., out of city trips, travels, etc.) • Be careful with your passwords; make them complex • Do NOT auto logon to social media

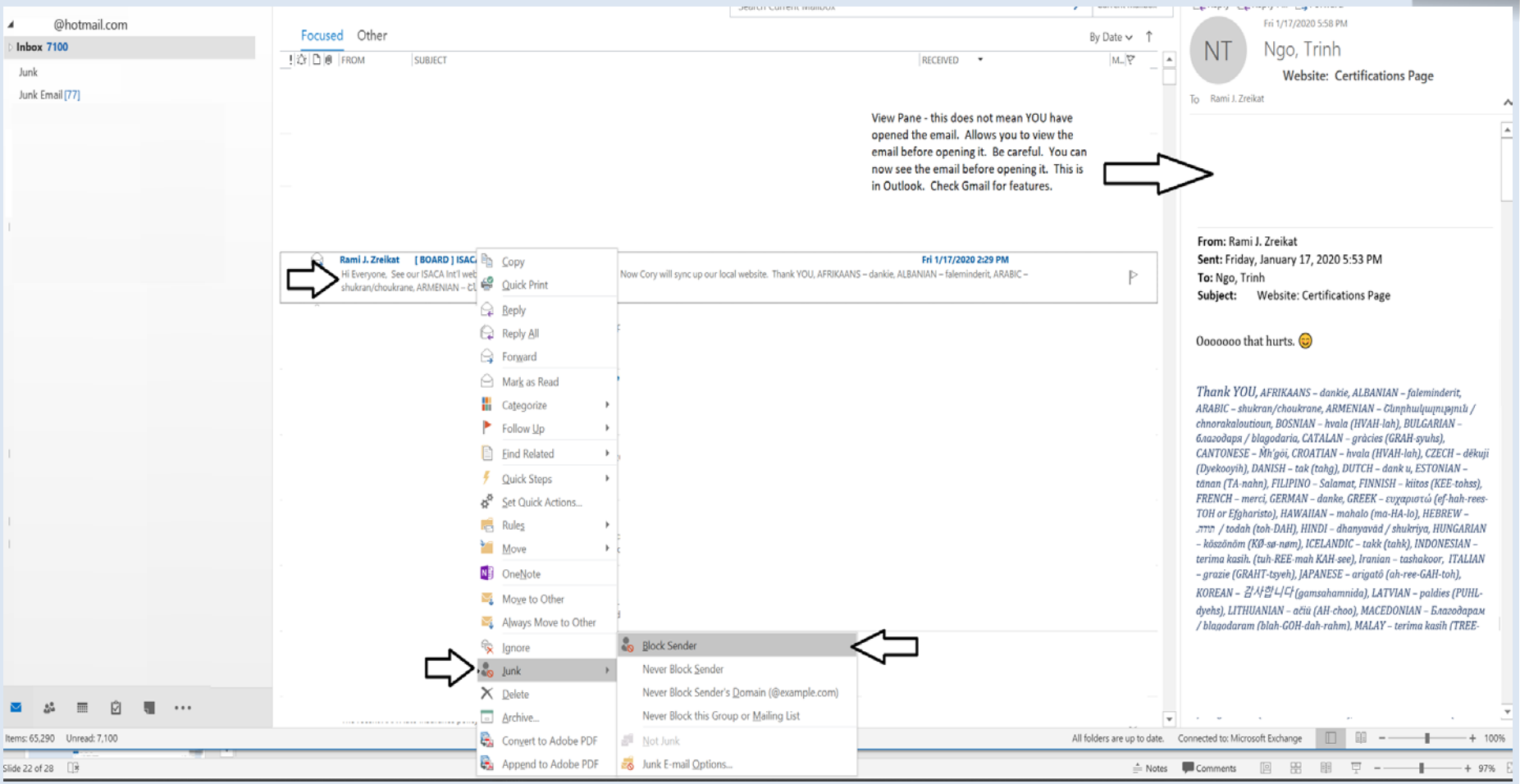
Preventable Measures

Cont'd

Use Case	Recommendation
Public WIFI (e.g., Starbucks©)	• Review the hotspot link to make sure it is legitimate • Surf only the Internet • Do NOT log on to your social media • Do NOT log on to you financial accounts • Do NOT log on to your email account • Use a personal VPN on your laptop to surf the Internet • Use your own mobile hotspot or buy a hotspot
Mobile Apps (e.g., Bank Access)	• It's ok as long as you use the bank's app • Ensure you subscribe to a second factor pin (e.g., authentication via a phone, phone call, or email for verification) • Do NOT use the iPhone Browser to log on to banks
Scam Calls	• Microsoft does not call you to resolve computer issues • IRS, EDD, FTB or any legitimate government agency will not call you with threats. You will receive letters first
Online Shopping	• Use strong Password • Use second factor authentication (e.g., email of a pin to your phone) for verification • Use PayPal for shopping and/or sign up for fraud protection with your Credit Card

Preventable Measures

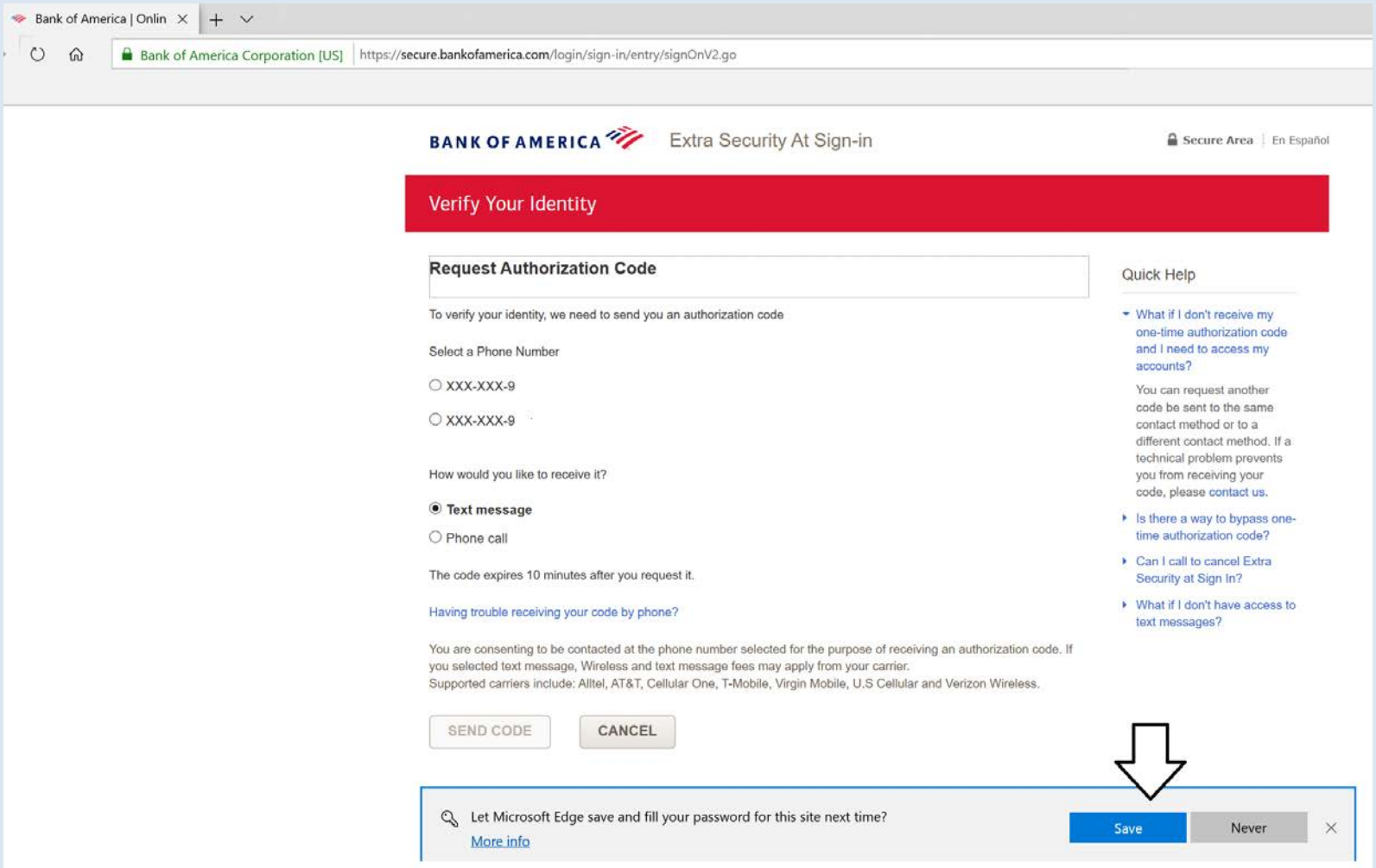
Cont'd



Mark as JUNK (Microsoft Outlook©) otherwise Press Hold SHIFT + DELETE keys.

Preventable Measures

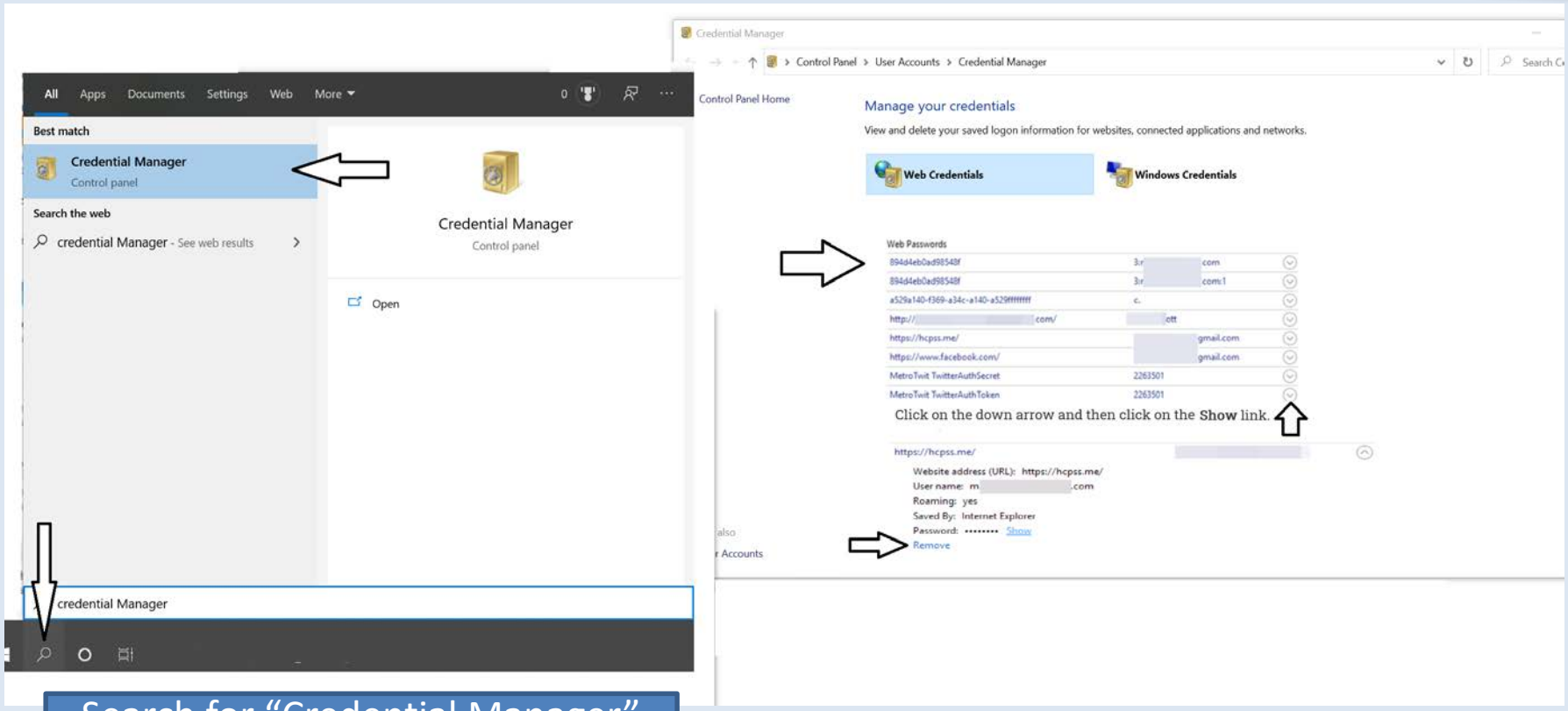
Cont'd



Never save your password on YOUR computer.

Preventable Measures

Cont'd

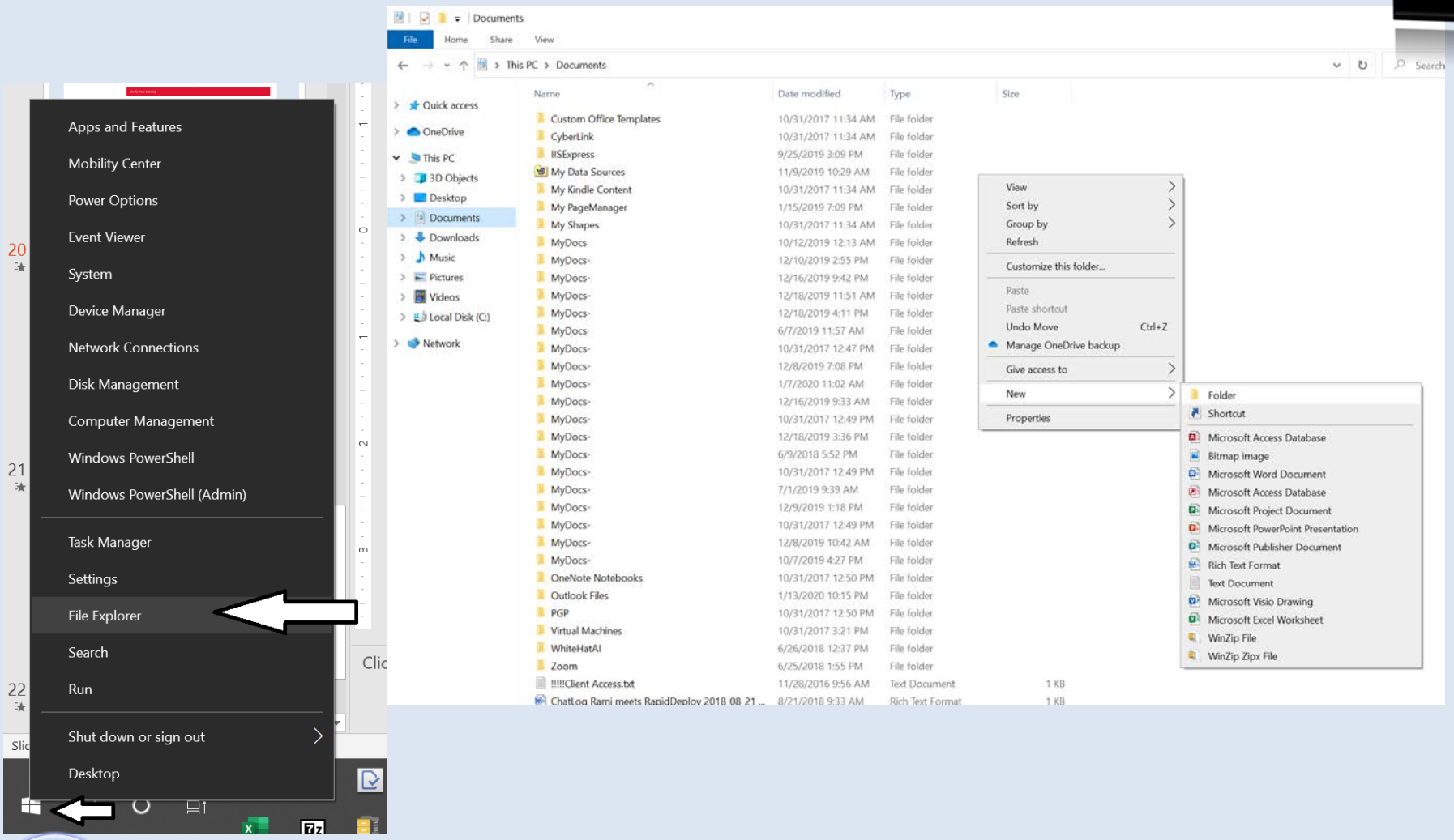


Search for "Credential Manager"

DELETE All saved user credentials; Windows10©

Preventable Measures

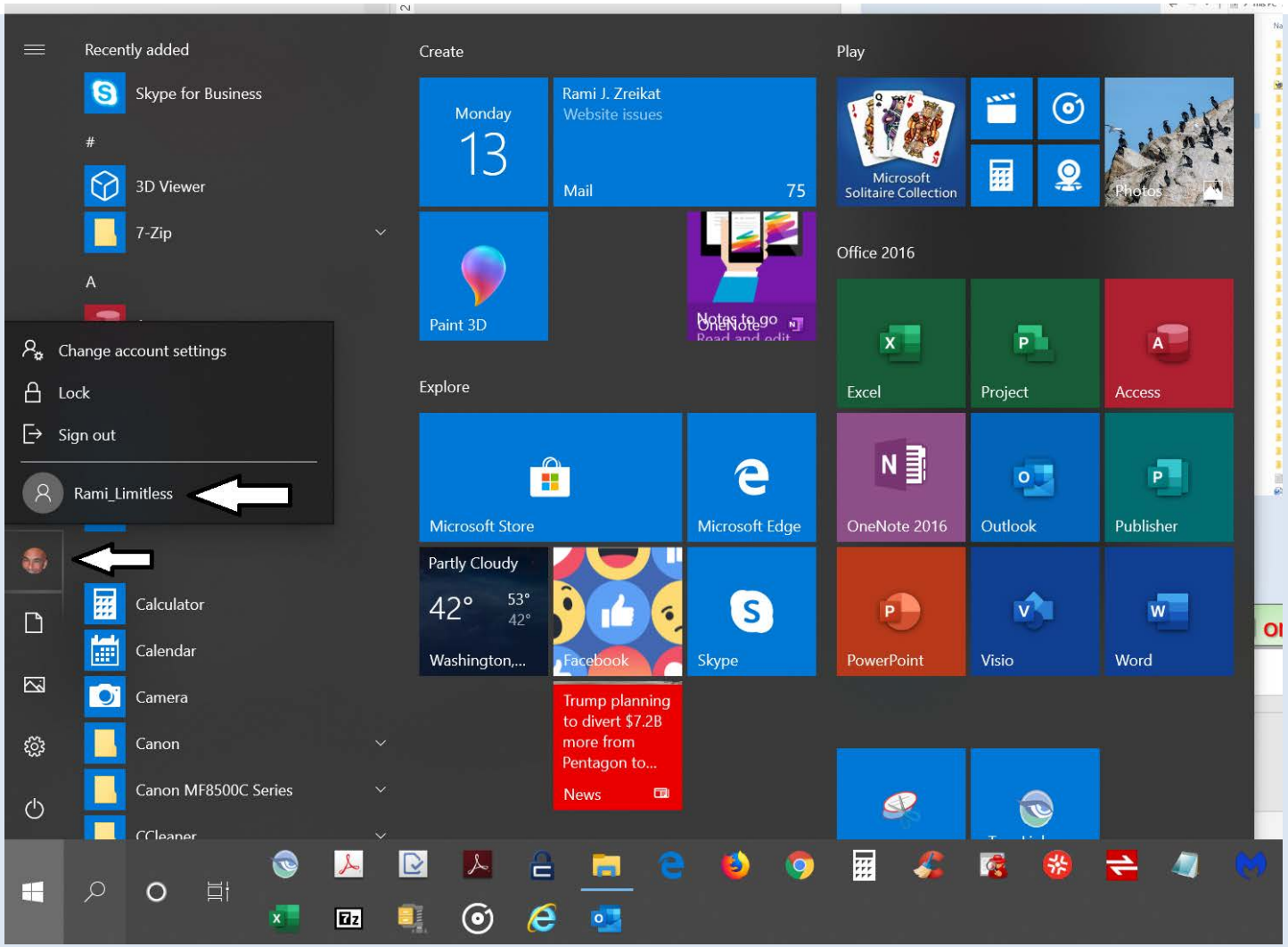
Cont'd



Structure your folders and organize them under "Documents" Put others in Downloads.

Preventable Measures

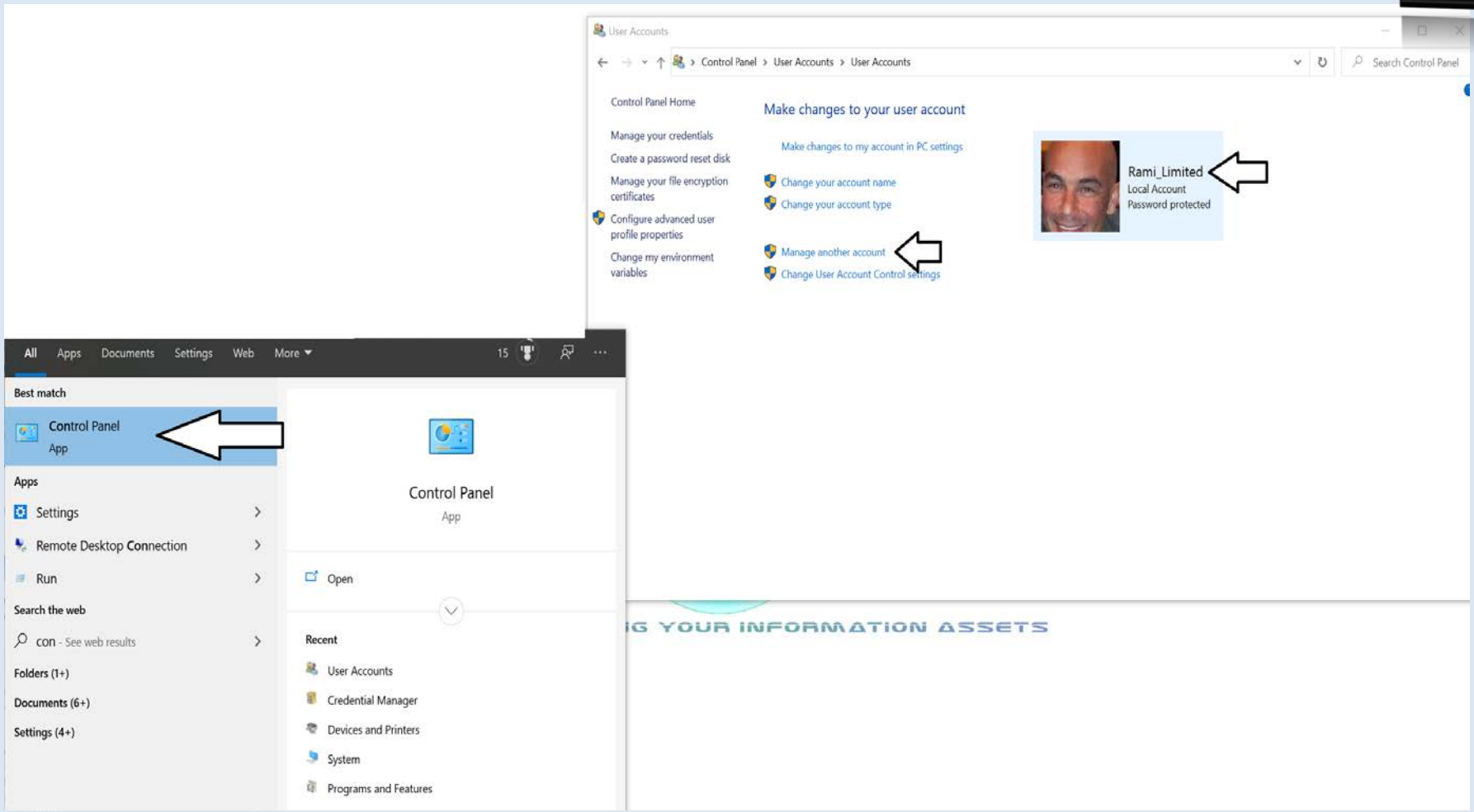
Cont'd



Create Two User Accounts – and sign in with "Standard User" Account

Preventable Measures

Cont'd



Create Two User Accounts – and sign in with "Standard User" Account

XTERRALINK

Public Sector, Private and Healthcare Divisions

903 Fulton Ave. Suite 408

Sacramento, CA 95825

https://www.xterralink.com/contact-us

CMAS: 3-12-70-2916a

(888) 444-9995

SB Micro: #1739057

"White Shark Kayak 140 MB Scan b-®Thomas P. Peschak.jpg"