



*Public Sector, Private and Healthcare Divisions*

## Security Hygiene Education Brief

The VERY FEW Steps to protect YOURSELF 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

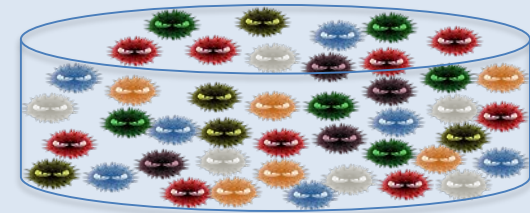


# Believe



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 accidentally?*



# 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. zinich
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?*

Google comcast router password

All Images News Videos Shopping More Settings Tools

About 1,010,000 results (0.50 seconds)

Open your browser and type 10.0. 0.1 in the address bar. You will be presented with a login screen. Type in the default username "admin" and the password will be "password" - then click LOGIN.

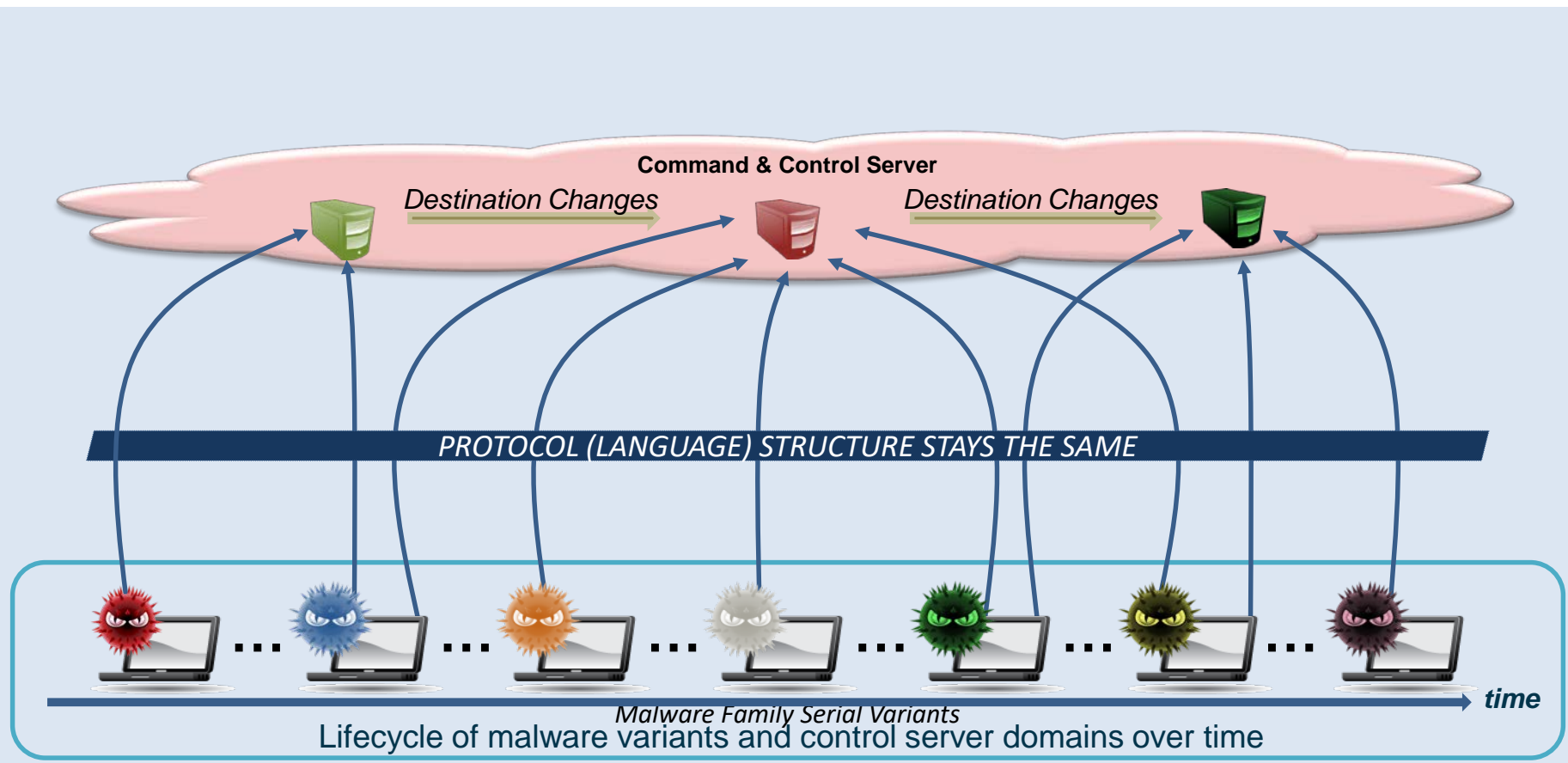
www.support.com > how-to > how-to-restore-my-xfinity-modem-11829  
How to Restore My Xfinity Modem - Support.com

Forgot to set remember manage

About Featured Snippets Feedback

- *Top 10 used Passwords in 2019 are ...*

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



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

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

Source: Damballa





# It Really Happens – Scenarios



The next set of scenarios 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.

Office365 Test



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.

**Bank Scam**



**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.

IRS Scam



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.

Ransomware



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.

Credentials



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.

Fake Pop Ups



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.

Fake Pop Ups



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.*

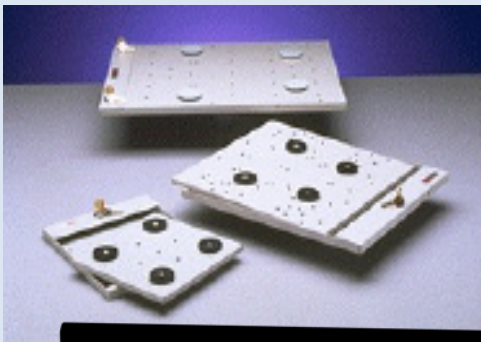
**Install Software**



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



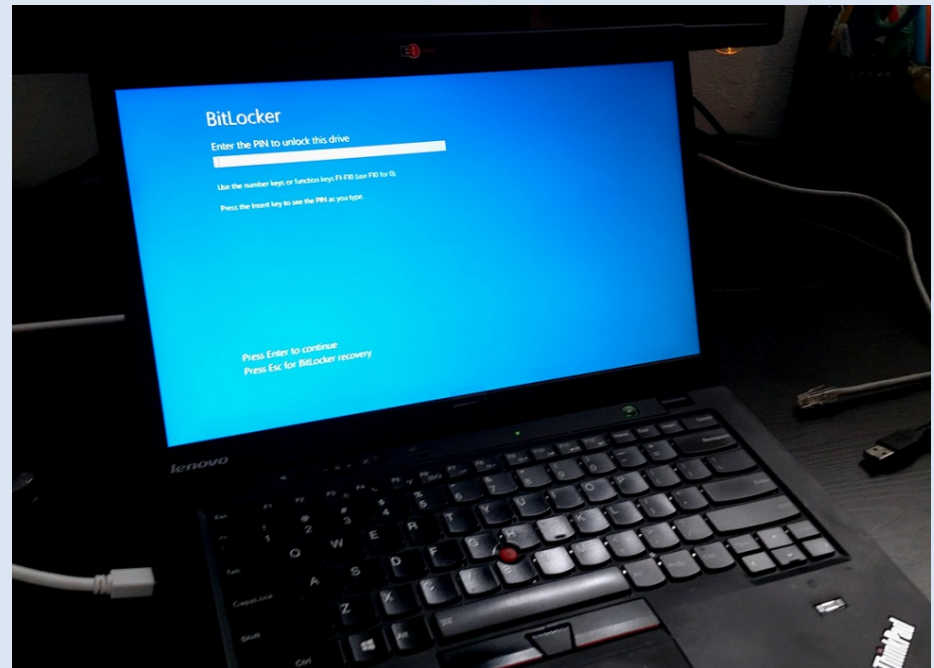
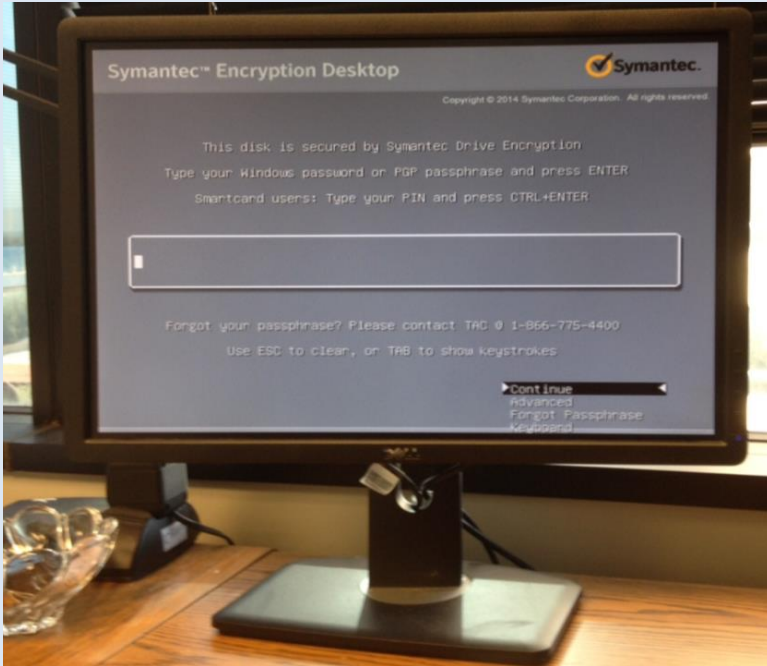
# Preventable Measures



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

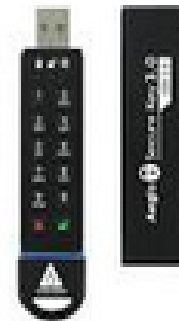
Best Buy



IronKey  
Enterprise D2...

\$109.99

CDW



Aegis Secure  
Key 3.0 240G...

\$369.00

Apricom



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 professional 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 your 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

View Pane - this does not mean YOU have opened the email. Allows you to view the email before opening it. Be careful. You can now see the email before opening it. This is in Outlook. Check Gmail for features.

**From:** Rami J. Zreikat  
**Sent:** Friday, January 17, 2020 5:53 PM  
**To:** Ngo, Trinh  
**Subject:** Website: Certifications Page

Ooooooooo that hurts. 😊

*Thank YOU, AFRIKAANS - dankie, ALBANIAN - faleminderit, ARABIC - shukran/choukrane, ARMENIAN - Շնորհակալություն / chnorakaloutioun, BOSNIAN - hvala (HVAH-lah), BULGARIAN - благодаря / blagodaria, CATALAN - gràcies (GRAH-syuh), CANTONESE - Mh'gái, CROATIAN - hvala (HVAH-lah), CZECH - děkuji (Dyekooyih), DANISH - tak (tahg), DUTCH - dank u, ESTONIAN - tänan (TA-nahn), FILIPINO - Salamat, FINNISH - kiitos (KEE-tohs), FRENCH - merci, GERMAN - danke, GREEK - ευχαριστώ (ef-hah-rees-TOH or Efgharisto), HAWAIIAN - mahalo (ma-HA-lo), HEBREW - תודה / todah (toh-DAH), HINDI - dhanyavad / shukriya, HUNGARIAN - köszönöm (KÖ-sh-nóm), ICELANDIC - takk (tahk), INDONESIAN - terima kasih, (tah-REE mah KAH-see), Iranian - tashakoor, ITALIAN - grazie (GRAHT-tsyeh), JAPANESE - arigatō (ah-ree-GAH-toh), KOREAN - 감사합니다 (gamsahamnida), LATVIAN - paldies (PUHL-dyehs), LITHUANIAN - ačiū (AH-choo), MACEDONIAN - Благодарам / blagodaram (blah-GOH-dah-rahm), MALAY - terima kasih (TREE-*

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

# Preventable Measures

Cont'd

The screenshot shows a web browser window with the Bank of America login page. The page title is "Bank of America | Online" and the URL is "https://secure.bankofamerica.com/login/sign-in/entry/signOnV2.g0". The page header includes the Bank of America logo, "Extra Security At Sign-in", and "Secure Area | En Español".

The main content area is titled "Verify Your Identity" and contains a "Request Authorization Code" form. The form includes a text input field, a "Quick Help" section with links to FAQs, and a "SEND CODE" button. A white arrow points from the "SEND CODE" button to a Microsoft Edge password save prompt at the bottom of the page.

**Request Authorization Code**

To verify your identity, we need to send you an authorization code

Select a Phone Number

XXX-XXX-9

XXX-XXX-9

How would you like to receive it?

Text message

Phone call

The code expires 10 minutes after you request it.

Having trouble receiving your code by phone?

You are consenting to be contacted at the phone number selected for the purpose of receiving an authorization code. If you selected text message, Wireless and text message fees may apply from your carrier. Supported carriers include: Alltel, AT&T, Cellular One, T-Mobile, Virgin Mobile, U.S Cellular and Verizon Wireless.

**Quick Help**

- What if I don't receive my one-time authorization code and I need to access my accounts?  
You can request another code be sent to the same contact method or to a different contact method. If a technical problem prevents you from receiving your code, please contact us.
- Is there a way to bypass one-time authorization code?
- Can I call to cancel Extra Security at Sign In?
- What if I don't have access to text messages?

Let Microsoft Edge save and fill your password for this site next time?  
[More info](#)

Never save your password on YOUR computer.

# Preventable Measures

Cont'd

The image shows two overlapping screenshots from a Windows 10 desktop. The left screenshot shows the Windows Start menu search interface. A search for "Credential Manager" has been performed, and the results show "Credential Manager" as the best match. A white arrow points to the "Credential Manager" result. Another white arrow points to the search bar at the bottom of the Start menu. The right screenshot shows the "Credential Manager" control panel window. It displays "Manage your credentials" with sections for "Web Credentials" and "Windows Credentials". Under "Web Credentials", there is a list of saved web passwords. A white arrow points to the "Web Passwords" section. Another white arrow points to the "Show" link next to a password entry. A third white arrow points to the down arrow icon next to the same password entry.

Search for "Credential Manager"

**DELETE All saved user credentials; Windows10©**

# Preventable Measures

Cont'd

20

21

22

File Explorer

Documents

Name	Date modified	Type	Size
Custom Office Templates	10/31/2017 11:34 AM	File folder	
CyberLink	10/31/2017 11:34 AM	File folder	
IISExpress	9/25/2019 3:09 PM	File folder	
My Data Sources	11/9/2019 10:29 AM	File folder	
My Kindle Content	10/31/2017 11:34 AM	File folder	
My PageManager	1/15/2019 7:09 PM	File folder	
My Shapes	10/31/2017 11:34 AM	File folder	
MyDocs	10/12/2019 12:13 AM	File folder	
MyDocs-	12/10/2019 2:55 PM	File folder	
MyDocs-	12/16/2019 9:42 PM	File folder	
MyDocs-	12/18/2019 11:51 AM	File folder	
MyDocs-	12/18/2019 4:11 PM	File folder	
MyDocs-	6/7/2019 11:57 AM	File folder	
MyDocs-	10/31/2017 12:47 PM	File folder	
MyDocs-	12/8/2019 7:08 PM	File folder	
MyDocs-	1/7/2020 11:02 AM	File folder	
MyDocs-	12/16/2019 9:33 AM	File folder	
MyDocs-	10/31/2017 12:49 PM	File folder	
MyDocs-	12/18/2019 3:36 PM	File folder	
MyDocs-	6/9/2018 5:52 PM	File folder	
MyDocs-	10/31/2017 12:49 PM	File folder	
MyDocs-	7/1/2019 9:39 AM	File folder	
MyDocs-	12/9/2019 1:18 PM	File folder	
MyDocs-	10/31/2017 12:49 PM	File folder	
MyDocs-	12/8/2019 10:42 AM	File folder	
MyDocs-	10/7/2019 4:27 PM	File folder	
OneNote Notebooks	10/31/2017 12:50 PM	File folder	
Outlook Files	1/13/2020 10:15 PM	File folder	
PGP	10/31/2017 12:50 PM	File folder	
Virtual Machines	10/31/2017 3:21 PM	File folder	
WhiteHatAI	6/26/2018 12:37 PM	File folder	
Zoom	6/25/2018 1:55 PM	File folder	
!!!!Client Access.txt	11/28/2016 9:56 AM	Text Document	1 KB
ChatLoa Rami meets RapidDeplov 2018 08 21 ...	8/21/2018 9:33 AM	Rich Text Format	1 KB

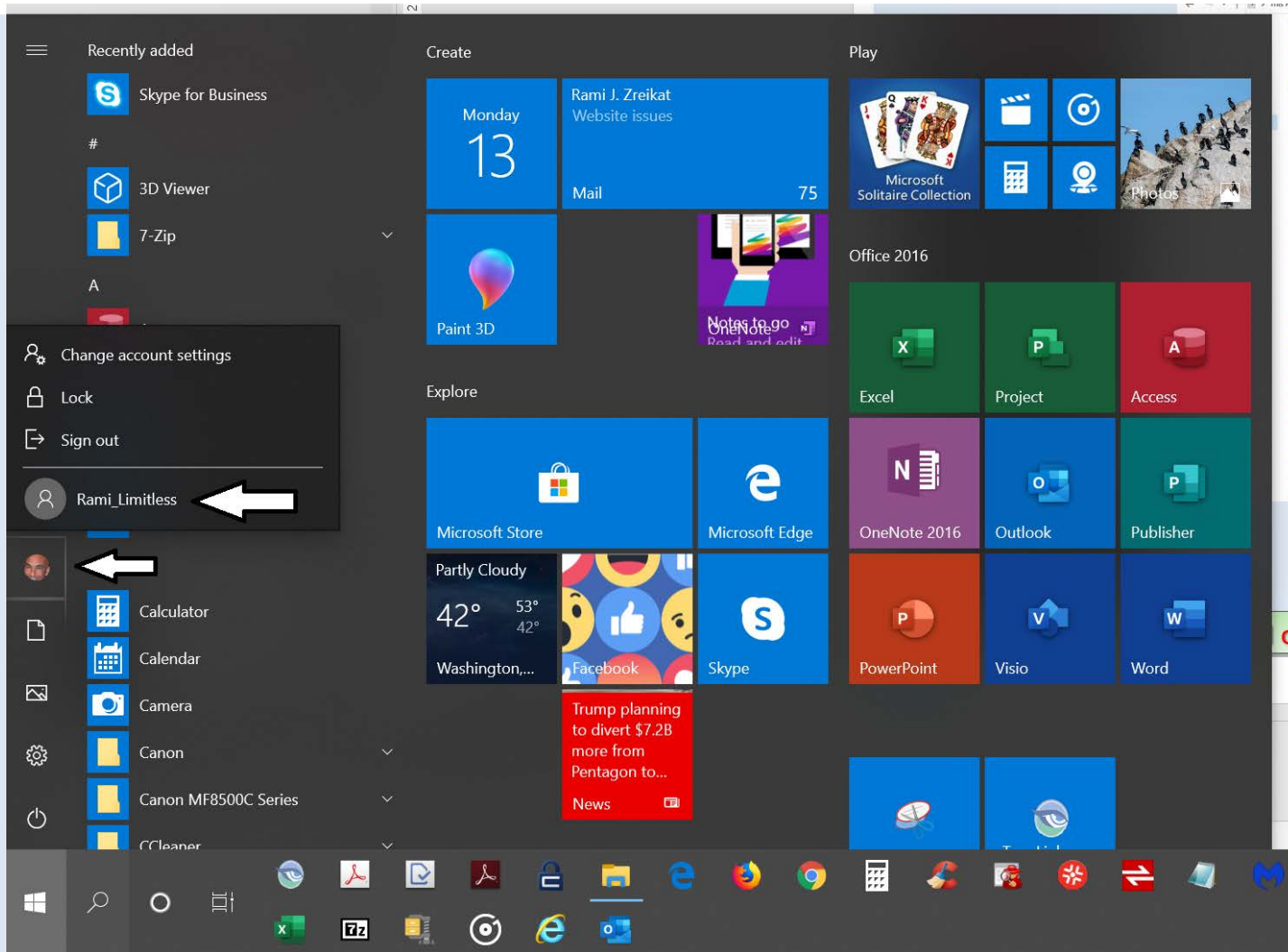
File Explorer context menu options:

- View
- Sort by
- Group by
- Refresh
- Customize this folder...
- Paste
- Paste shortcut
- Undo Move (Ctrl+Z)
- Manage OneDrive backup
- Give access to
- New
  - Folder
  - Shortcut
  - Microsoft Access Database
  - Bitmap image
  - Microsoft Word Document
  - Microsoft Access Database
  - Microsoft Project Document
  - Microsoft PowerPoint Presentation
  - Microsoft Publisher Document
  - Rich Text Format
  - Text Document
  - Microsoft Visio Drawing
  - Microsoft Excel Worksheet
  - WinZip File
  - WinZip Zipx File
- Properties

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

The image shows two overlapping windows from a Windows operating system. The top window is the 'User Accounts' control panel window. It displays options for managing user accounts, including 'Change your account name', 'Change your account type', 'Manage another account', and 'Change User Account Control settings'. A white arrow points to the 'Manage another account' option. To the right, a user profile card for 'Rami\_Limited' is shown, with another white arrow pointing to it. The bottom window is the Windows Start menu search interface. The search bar contains the text 'con'. The search results show 'Control Panel' as the best match, with a white arrow pointing to it. Below the search results, a list of recent items is visible, including 'User Accounts', 'Credential Manager', 'Devices and Printers', 'System', and 'Programs and Features'.

Create Two User Accounts – and sign in with “Standard User” Account



*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"