
PERSONAL CYBER SECURITY

DAVE CHRISTOPHERSON – HAUS TECHS

TOPICS

- ▶ What are the bad guys after?
- ▶ Where are you at risk?
- ▶ How are you at risk?
- ▶ How can you protect yourself?
- ▶ Q and A

WHAT ARE THE BAD GUYS AFTER?

- ▶ Immediate monetary gain
 - ▶ Ransomware
 - ▶ Support calls
 - ▶ Phishing and Whaling

TEXT

PHISHING AND WHALING

Alerts : Recent Changes In Your Account Activity.



U.S.Bank <noreplyalertsmaillsus8995@nyc.rr.com>

🔒 Undisclosed-Recipients;

Saturday, July 27, 2019 at 7:21 AM

[Show Details](#)



Action: Recent changes in your account activity

Date: 07/27/2019

Dear US Bank Customer,

We have detected irregular activity on your account. So we have limited your account. For your protection, you have to verify this activity before you can continue using your account.

Please [Click here](#) to remove any restrictions placed on your account.

Reference Number: US-558-107-163

Thank you for banking with us.

Sincerely,

U.S Bank Online Support

PHISHING AND WHALING

Suspicious Activity Detected On Your SunTrust

 **SunTrust Alert** <services_customers@hvc.rr.com>
Undisclosed-Recipients;
Friday, July 19, 2019 at 8:00 AM
[Show Details](#)

 This message is high priority.



Dear Customer,

We detected suspicious activity on your account and as result, for your security, we've temporarily suspended your account to protect your information and you need to verify your identity before you can continue using your account.

To re-activate your account, please "**Sign On**" now and verify your information to prevent any suspicious activities at once.


<https://u.to/Uz-jFQ>

Thank you for banking with SunTrust Bank.

Sincerely,
SunTrust Customer Care

SunTrust Bank, Member FDIC. ©2019 SunTrust Banks, Inc. SunTrust is a federally registered service mark of SunTrust Bank. This email was sent on behalf of SunTrust Customer Care.

PHISHING AND WHALING

Notice : Important Security Alert.



Bank Of America <noreplybofasystemenhanced776@tampabay.rr.com>

Undisclosed-Recipients;

Friday, July 19, 2019 at 5:46 AM

[Show Details](#)

! This message is high priority.



Security Alert: We have detected an action that seems to be unauthorized by the account owner

We're letting you know that we've detected some unusual activity on your Bank of America Account. It seems that one or more unauthorized devices was connected to your account.



What do i need to do ?

- We have not fully restricted your account but you must confirm your identity in order to avoid any deviations.
- For your protection, transactions on your account may be limited until you are able to confirm your identity.
- To better protect you against fraud, we are now using an Online Identification System to verify suspected fraud activities.

[Click here to verify your account](#)

- Failure to complete the validation process will result in a suspension of your Bank of America Account.

We take every step needed to automatically validate our users, unfortunately in this case we were unable to verify your details. The process will only take a couple of minutes and will allow us to maintain our high standard of account security.

Bank of America Support Team

Bank of America Email, NC1-028-09-01, 150 N College St., Charlotte, NC 28255.

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#)
© 2019 Bank of America Corporation. All rights reserved.

- ▶ Personal data for later gain or to market to others
- ▶ Hacking for fun
- ▶ Access to your home (IoT devices)
 - ▶ Cameras
 - ▶ Smart locks
 - ▶ Garage Doors etc.

WHERE ARE YOU AT RISK?

- ▶ Home network
 - ▶ Default settings password etc
 - ▶ Cheapest router is not the best router
 - ▶ Is your Wifi identifiable?
- ▶ In the wild
 - ▶ No network outside you house is a safe network

HOW ARE YOU AT RISK?

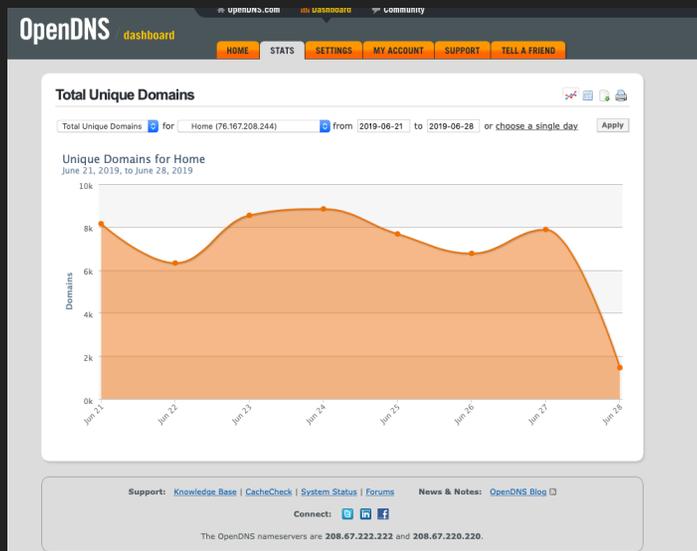
- ▶ Weak and common passwords

- ▶ 123456 (Unchanged)
- ▶ password (Unchanged)
- ▶ 123456789 (Up 3)
- ▶ 12345678 (Down 1)
- ▶ 12345 (Unchanged)
- ▶ 111111 (New)
- ▶ 1234567 (Up 1)
- ▶ sunshine (New)
- ▶ qwerty (Down 5)
- ▶ Iloveyou (Unchanged)

- ▶ Reusing Passwords

HOW TO PROTECT YOURSELF?

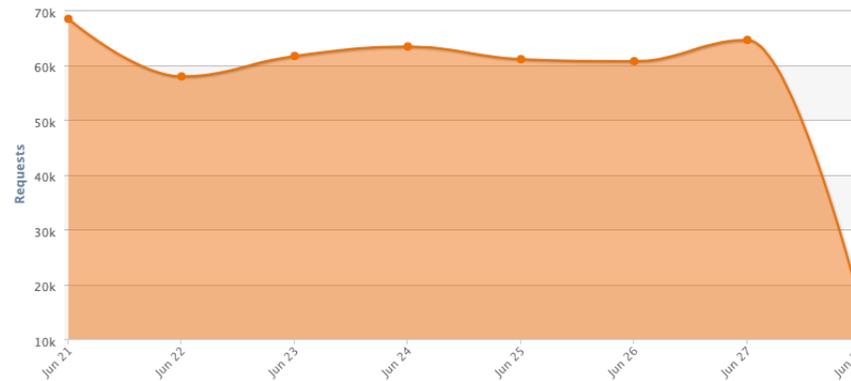
- ▶ Home network
 - ▶ Invest in a good router or firewall
 - ▶ Keep it updated
 - ▶ Use OpenDNS or other service



Total Requests

Total Requests for Home (76.167.208.244) from 2019-06-21 to 2019-06-28 or choose a single day Apply

Total Requests for Home
June 21, 2019, to June 28, 2019



Support: [Knowledge Base](#) | [CacheCheck](#) | [System Status](#) | [Forums](#) News & Notes: [OpenDNS Blog](#)

Connect: [Twitter](#) [LinkedIn](#) [Facebook](#)

The OpenDNS nameservers are 208.67.222.222 and 208.67.220.220.

Domains

Domains for Home (76.167.208.244) from 2019-06-21 to 2019-06-28 or choose a single day Apply

Filter: View everything

Next →

RANK	DOMAIN	REQUESTS
1	softwareupdate.vmware.com	105,274
2	auth.gfx.ms	51,638
3	home146-my.sharepoint.com	38,552
4	*.local	25,333
5	dzt-mcs-amzn-us-east-1-h0m3.upe.p.hmr.sophos.com	14,972
6	login.microsoftonline.com	13,888
7	login.windows.net	12,945
8	login.microsoft.com	12,788
9	es.ring.com	10,444
10	*.amazonaws.com	9,353
11	ami-gateway-adapter.enertalk.com	8,225
12	*.akamaiedge.net	6,319
13	strict.bing.com	4,999
14	*.cloudfront.net	4,688
15	gmail.com	4,480
16	pool.ntp.org	4,222

Web Content Filtering

Choose your filtering level

- High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.
28 categories in this group - [View](#) - [Customize](#)
- Moderate** Protects against all adult-related sites and illegal activity.
15 categories in this group - [View](#) - [Customize](#)
- Low** Protects against pornography.
6 categories in this group - [View](#) - [Customize](#)
- None** Nothing blocked.
- Custom** Choose the categories you want to block.

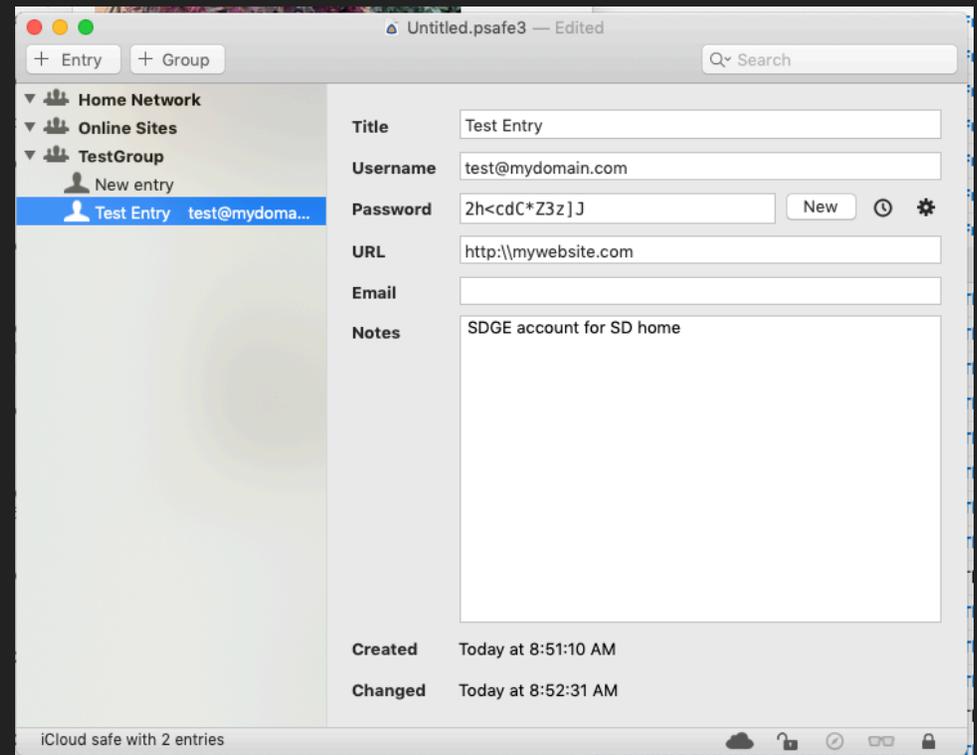
- | | | |
|--|--|--|
| <input type="checkbox"/> Academic Fraud | <input type="checkbox"/> Adult Themes | <input checked="" type="checkbox"/> Adware |
| <input type="checkbox"/> Alcohol | <input type="checkbox"/> Anime/Manga/Webcomic | <input type="checkbox"/> Auctions |
| <input type="checkbox"/> Automotive | <input type="checkbox"/> Blogs | <input type="checkbox"/> Business Services |
| <input type="checkbox"/> Chat | <input type="checkbox"/> Classifieds | <input type="checkbox"/> Dating |
| <input type="checkbox"/> Drugs | <input type="checkbox"/> Ecommerce/Shopping | <input type="checkbox"/> Educational Institutions |
| <input type="checkbox"/> File Storage | <input type="checkbox"/> Financial Institutions | <input type="checkbox"/> Forums/Message boards |
| <input type="checkbox"/> Gambling | <input type="checkbox"/> Games | <input type="checkbox"/> German Youth Protection |
| <input type="checkbox"/> Government | <input type="checkbox"/> Hate/Discrimination | <input type="checkbox"/> Health and Fitness |
| <input type="checkbox"/> Humor | <input type="checkbox"/> Instant Messaging | <input type="checkbox"/> Jobs/Employment |
| <input type="checkbox"/> Lingerie/Bikini | <input type="checkbox"/> Movies | <input type="checkbox"/> Music |
| <input type="checkbox"/> News/Media | <input type="checkbox"/> Non-Profits | <input type="checkbox"/> Nudity |
| <input type="checkbox"/> P2P/File sharing | <input type="checkbox"/> Parked Domains | <input type="checkbox"/> Photo Sharing |
| <input type="checkbox"/> Podcasts | <input type="checkbox"/> Politics | <input type="checkbox"/> Pornography |
| <input type="checkbox"/> Portals | <input checked="" type="checkbox"/> Proxy/Anonymizer | <input type="checkbox"/> Radio |
| <input type="checkbox"/> Religious | <input type="checkbox"/> Research/Reference | <input type="checkbox"/> Search Engines |
| <input type="checkbox"/> Sexuality | <input type="checkbox"/> Social Networking | <input type="checkbox"/> Software/Technology |
| <input type="checkbox"/> Sports | <input type="checkbox"/> Tasteless | <input type="checkbox"/> Television |
| <input type="checkbox"/> Tobacco | <input type="checkbox"/> Travel | <input type="checkbox"/> Video Sharing |
| <input type="checkbox"/> Visual Search Engines | <input type="checkbox"/> Weapons | <input checked="" type="checkbox"/> System Preferences |

HOW TO PROTECT YOURSELF?

- ▶ Keep all computers/phones/tablets/cameras/streaming devices/doorbells etc updated
- ▶ Change default passwords of all your devices!
- ▶ Turn on auto update
- ▶ Backup your data to a local or cloud device
- ▶ Carbonite, iCloud, OneDrive
- ▶ Use a good Ransomware/virus software with rollback if possible (Sophos, Microsoft)
- ▶ Separate your IoT traffic from your computers if possible
- ▶ Outside your home
 - ▶ Use your smart phone as a hotspot or use a MIFI device.
 - ▶ Use a VPN if you have to connect to bank, 401K etc.

HOW TO PROTECT YOURSELF?

- ▶ STOP Reusing Passwords
- ▶ Switch to Complex passwords
 - ▶ 8,lLsb<#dC6v
- ▶ Password Managers



- ▶ Microsoft, Apple, Google and IRS aren't going to call you offering help.
- ▶ Keep yourself informed subscribe to computer security blogs or email lists.

QUESTIONS?