Questions, Issues,

Concerns, Suggestions

Welcome at any time

Even Now

Sun City Computer Club

Cyber Security SIG

June 7, 2018

SCCCCyber@gmail.com

Current Issues

- VPNFilter
- GDPR
- “BackSwap” banking trojan
- Echo fuzzy match

Top Cyber Security items

- 3-2-1 Backup
- Cloud Care
  Know what, when, where, why, who
- Inventory
  How many computers do you have?
  Applications, Accounts, Backups, …
- Tape over camera lenses
- Sound – Frequency
- Quad 9 DNS servers everywhere
- Administrator
- Encryption – dual edged sword
- Do not click

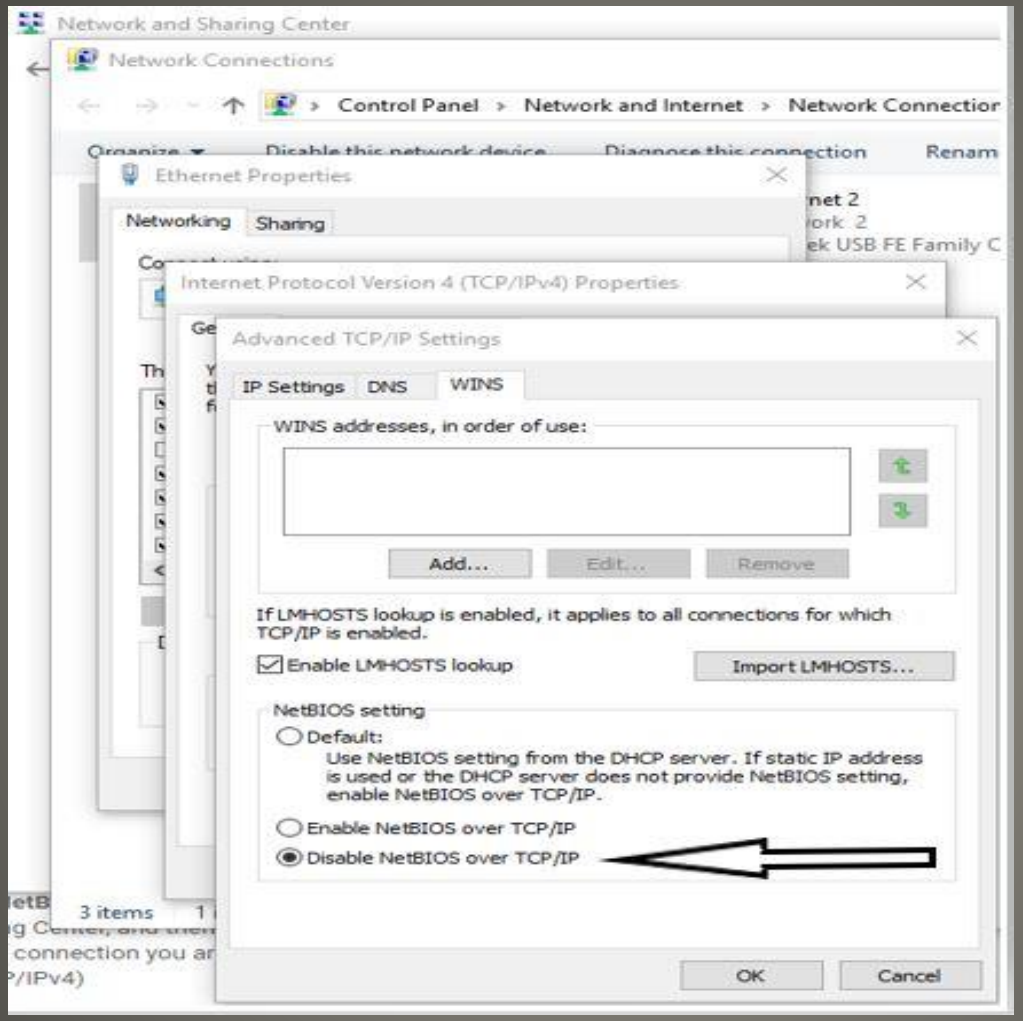
- Seriously Do Not Click

  - Hover over
  - Copy and Paste to more secure environment
  - Research

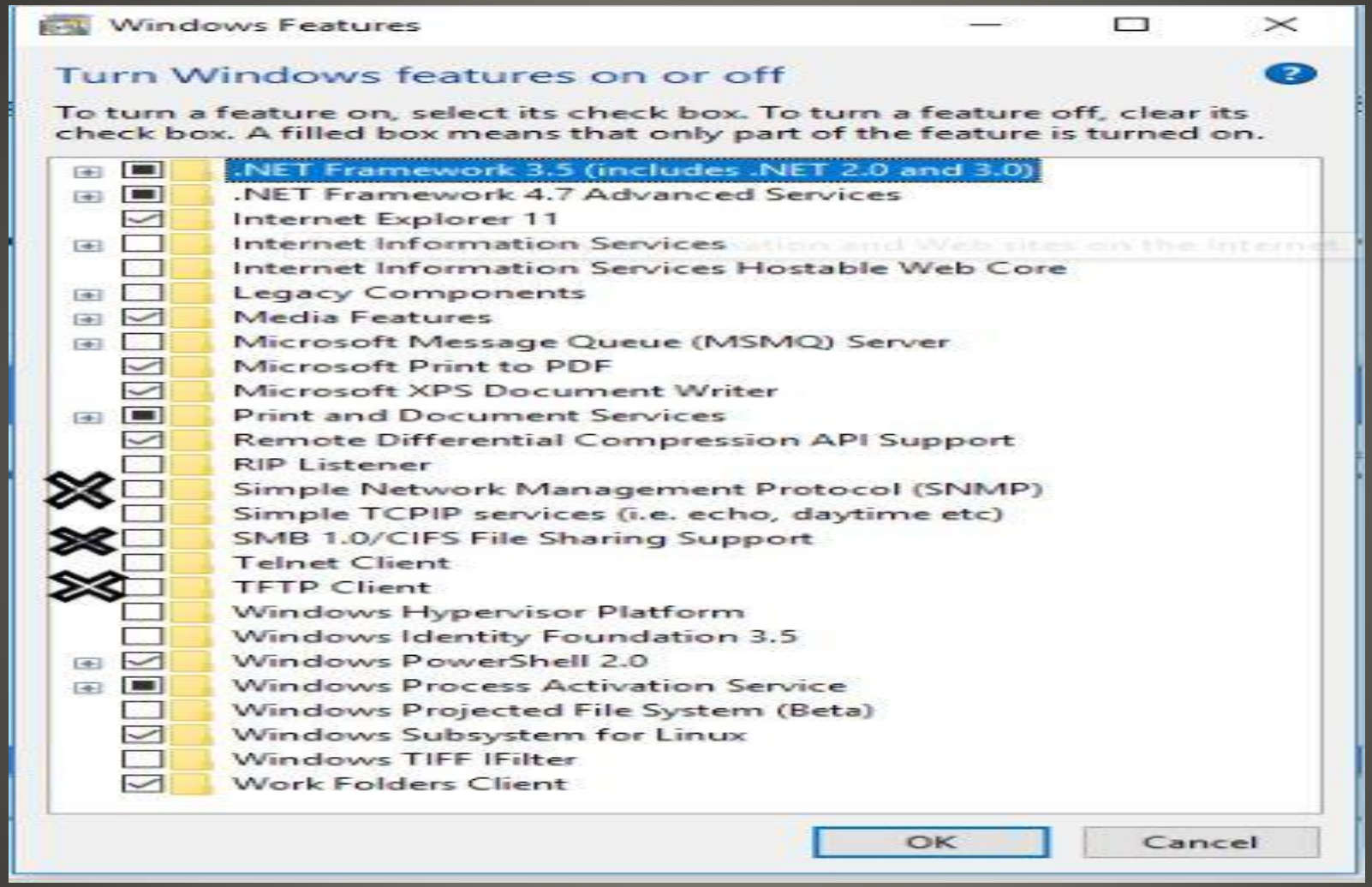
Do Not Click

Multiple

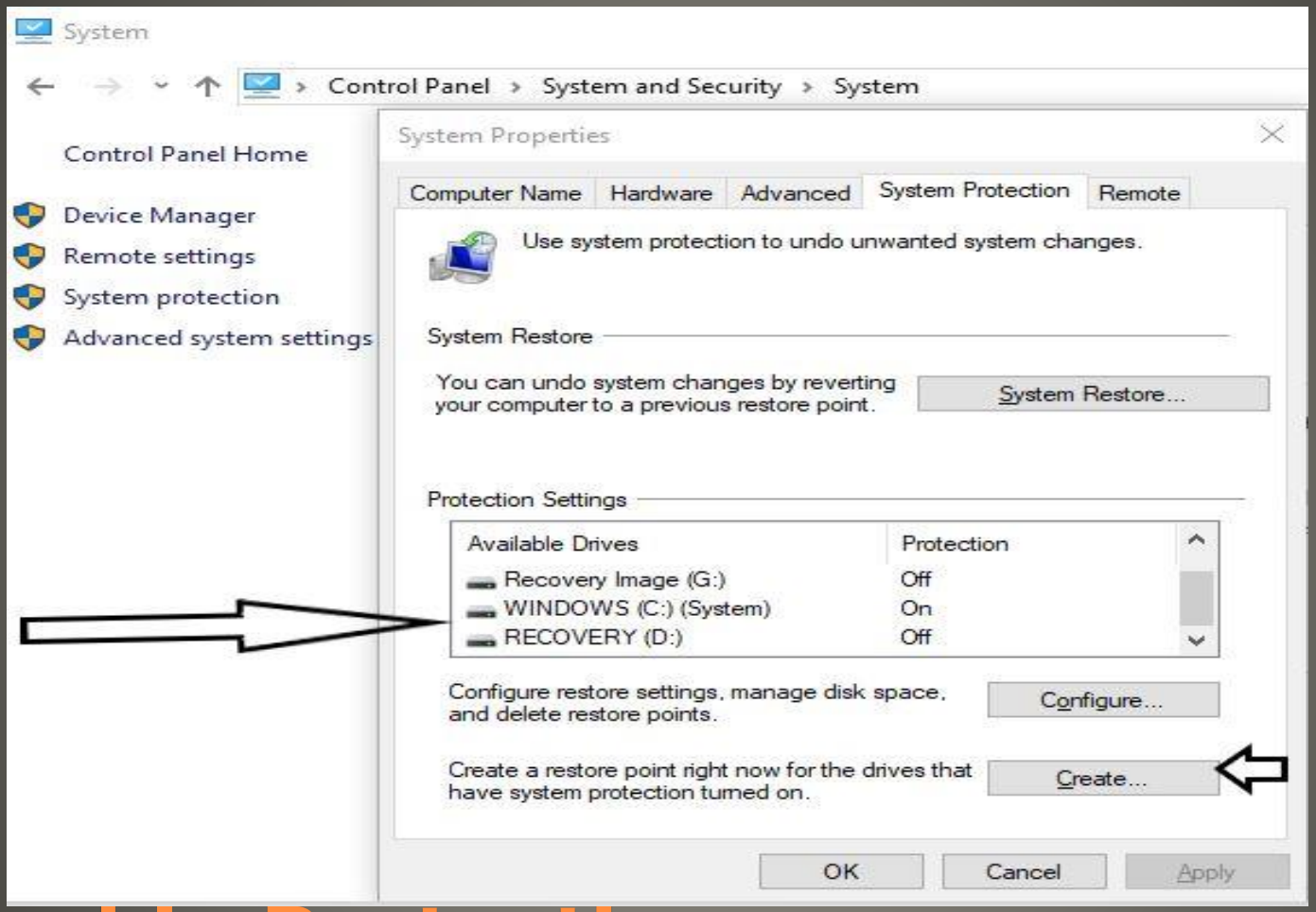
- Browsers
- Devices
- eMail addresses
- IDentities
- Phone numbers



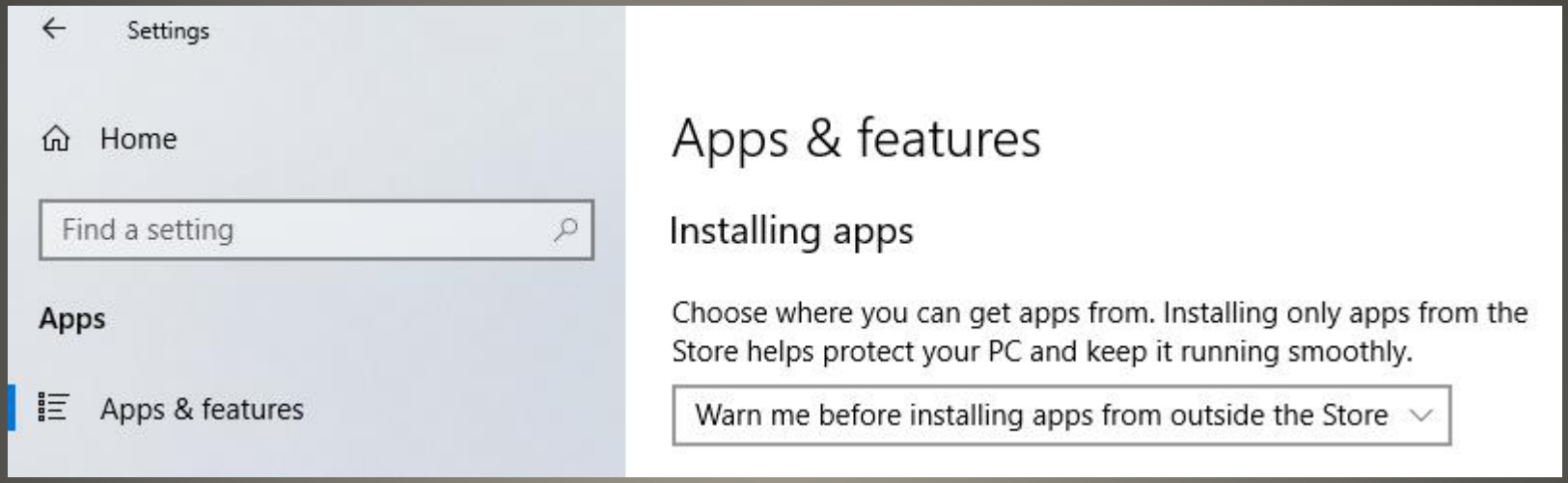
Disable NetBIOS over TCPIP



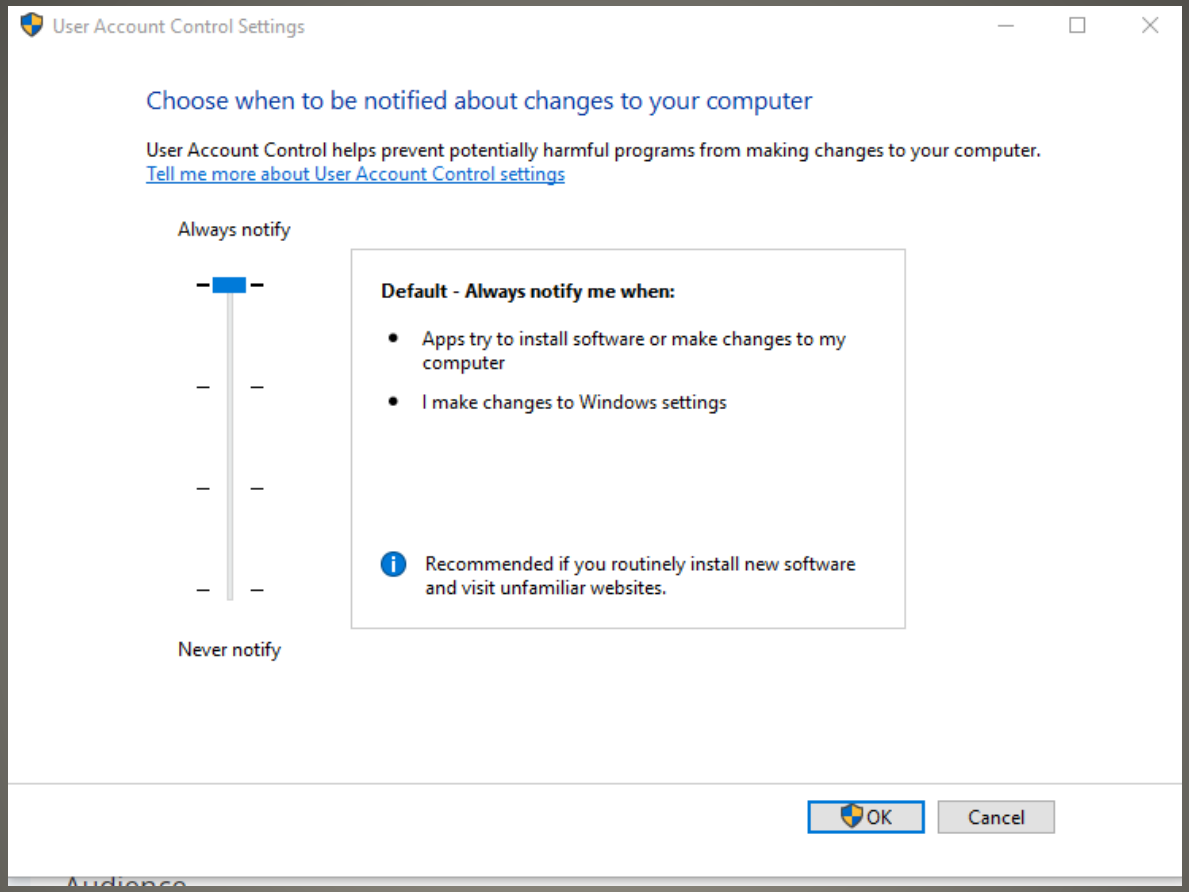
Windows Features



Enable Protection
Create restore point



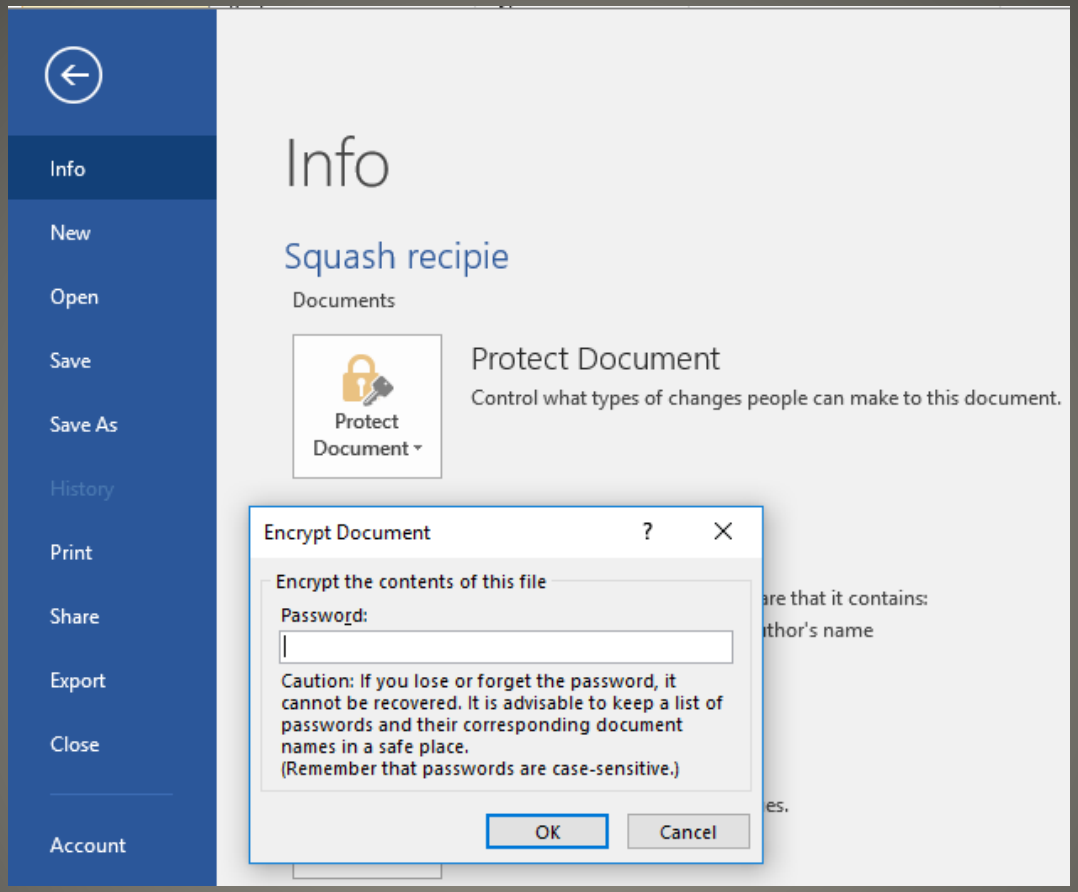
Apps not from store warning



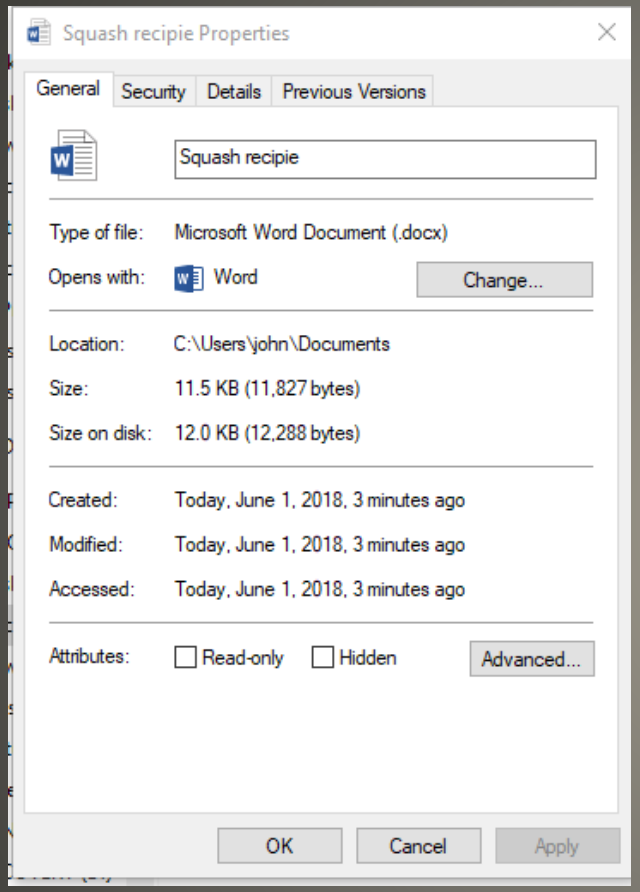
User Access Control

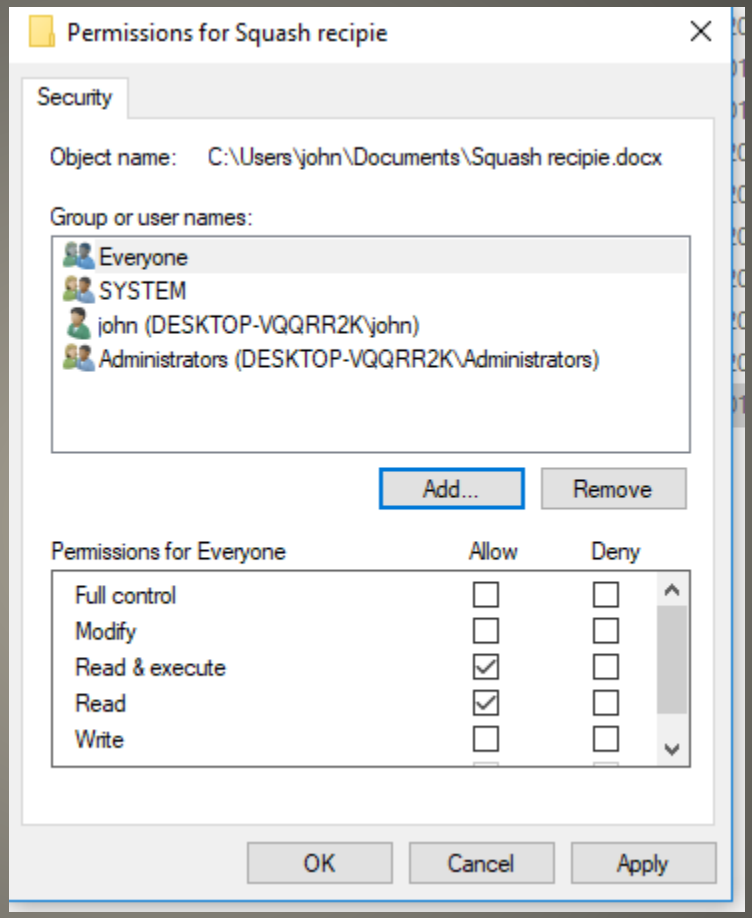
- Recovery point & Backup
- Bloatware remove
- Startup review
- windows.old folder
- File and Folder permissions

Top Cyber Security Items



Protect sensitive documents



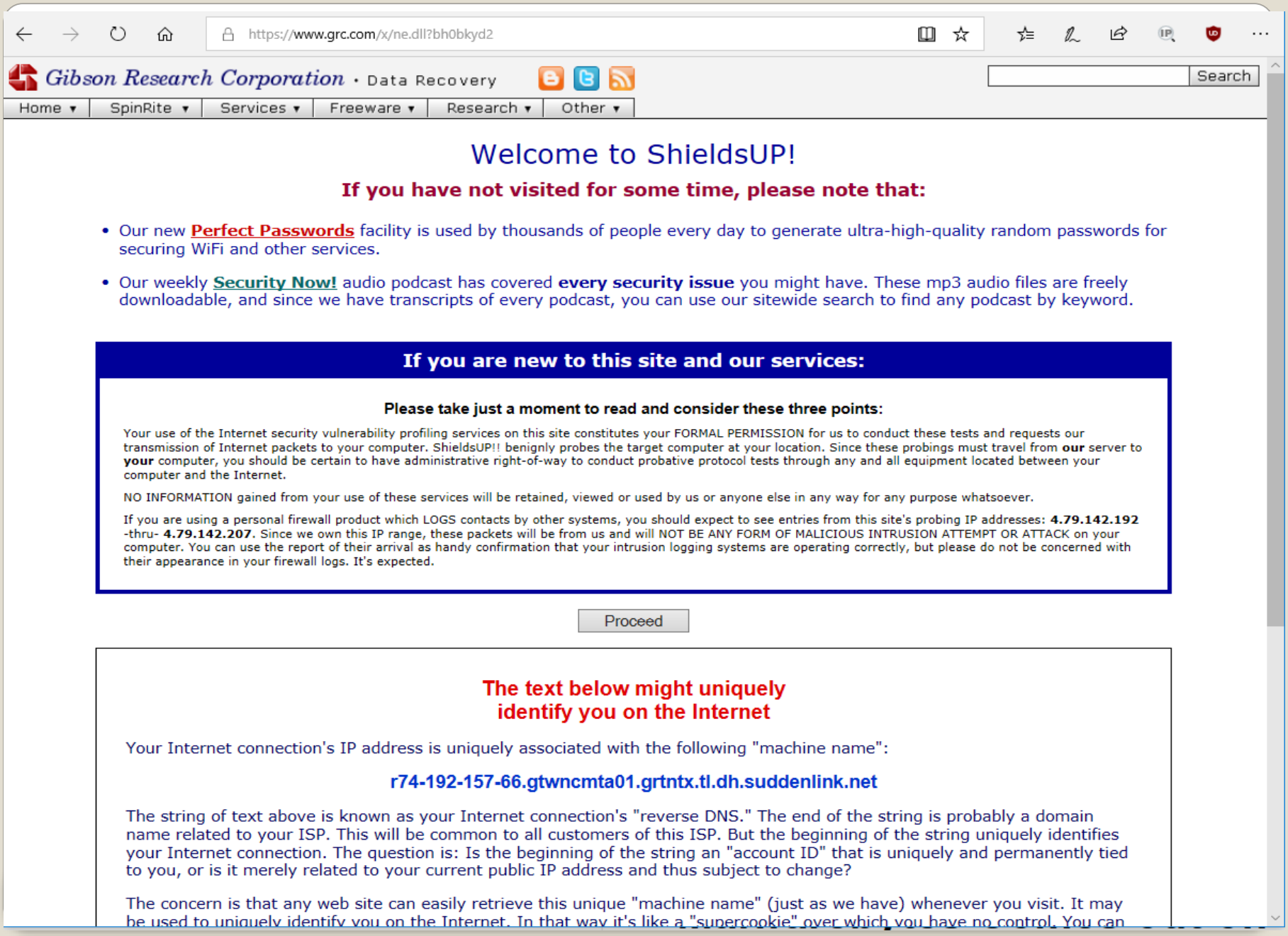


Protect sensitive documents

Home Network

- Segmentation Wi-Fi Guest
- Firewalls On
- Monitor
- Off when not needed lose lease
- Radio

  SSID, Strong passphrase, disable remote administration, firmware updates, monitor
- ShieldsUp!


https://www.grc.com/x/ne.dll?bh0bkyd2
Gibson Research Corporation • Data Recovery
Search
Home
SpinRite
Services
Freeware
Research
Other
Welcome to ShieldsUP!
If you have not visited for some time, please note that:
Our new Perfect Passwords facility is used by thousands of people every day to generate ultra-high-quality random passwords for securing WiFi and other services.
Our weekly Security Now! audio podcast has covered every security issue you might have. These mp3 audio files are freely downloadable, and since we have transcripts of every podcast, you can use our sitewide search to find any podcast by keyword.
If you are new to this site and our services:
Please take just a moment to read and consider these three points:
Your use of the Internet security vulnerability profiling services on this site constitutes your FORMAL PERMISSION for us to conduct these tests and requests our transmission of Internet packets to your computer. ShieldsUP!! benignly probes the target computer at your location. Since these probings must travel from our server to your computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet.
NO INFORMATION gained from your use of these services will be retained, viewed or used by us or anyone else in any way for any purpose whatsoever.
If you are using a personal firewall product which LOGS contacts by other systems, you should expect to see entries from this site's probing IP addresses: 4.79.142.192 -thru- 4.79.142.207. Since we own this IP range, these packets will be from us and will NOT BE ANY FORM OF MALICIOUS INTRUSION ATTEMPT OR ATTACK on your computer. You can use the report of their arrival as handy confirmation that your intrusion logging systems are operating correctly, but please do not be concerned with their appearance in your firewall logs. It's expected.
Proceed
The text below might uniquely identify you on the Internet
Your Internet connection's IP address is uniquely associated with the following "machine name":
r74-192-157-66.gtwncmta01.grtntx.tl.dh.suddenlink.net
The string of text above is known as your Internet connection's "reverse DNS." The end of the string is probably a domain name related to your ISP. This will be common to all customers of this ISP. But the beginning of the string uniquely identifies your Internet connection. The question is: Is the beginning of the string an "account ID" that is uniquely and permanently tied to you, or is it merely related to your current public IP address and thus subject to change?
The concern is that any web site can easily retrieve this unique "machine name" (just as we have) whenever you visit. It may be used to uniquely identify you on the Internet. In that way it's like a "supercookie" over which you have no control. You can

https://www.grc.com/x/ne.dll?rh1dkyd2

Gibson Research Corporation · Security

Search

Home ▾ | SpinRite ▾ | Services ▾ | Freeware ▾ | Research ▾ | Other ▾

ShieldsUP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Greetings!

Without your knowledge or explicit permission, the Windows networking technology which connects your computer to the Internet **may be offering some or all of your computer's data to the entire world at this very moment!**

- **For orientation and background,** please examine the page links provided below for important information about Internet vulnerabilities, precautions and solutions.
- **First time users** should start by checking their **Windows File Sharing** and **Common Ports** vulnerabilities with the "File Sharing" and "Common Ports" buttons below.
- For orientation and information about the Port Authority system, **click the Home or Help icons** in the titlebar . . .

Click here to check your router now...

GRC's Instant UPnP Exposure Test

HOME | **ShieldsUP!! Services** | HELP

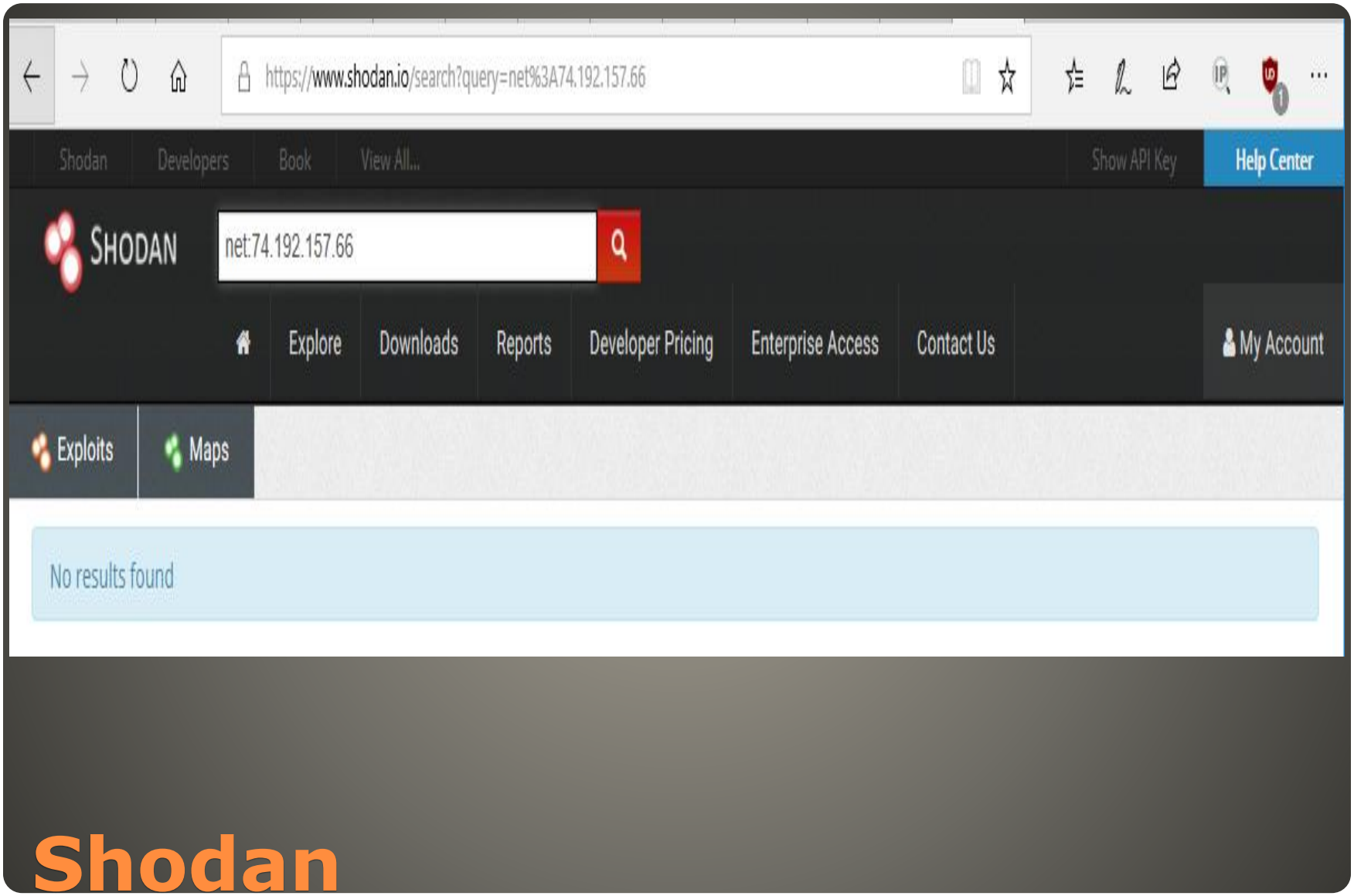
File Sharing	Common Ports	All Service Ports	Messenger Spam	Browser Headers

You may select any service from among those listed above . . .

User Specified Custom Port Probe	Lookup Specific Port Information

Or enter a port to lookup, or the ports for a custom probe to check, then choose the service. Your computer at IP 74.192.157.66 will be tested.


https://www.grc.com/x/ne.dll?rh1dkyd2
Gibson Research Corporation • Data Recovery
Search
Home
SpinRite
Services
Freeware
Research
Other
ShieldsUP!!
Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson, Gibson Research Corporation.
Universal Plug n'Play (UPnP)
Internet Exposure Test
This Internet probe sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets, one every half-second, to our visitor's current IPv4 address (74.192.157.66) in an attempt to solicit a response from any publicly exposed and listening UPnP SSDP service. The UPnP protocols were never designed to be exposed to the public Internet, and any Internet-facing equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.
Your equipment at IP:
74.192.157.66
Is now being queried:
THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!
(That's good news!)


https://www.shodan.io/search?query=net%3A74.192.157.66
Shodan
Developers
Book
View All...
Show API Key
Help Center
SHODAN
net:74.192.157.66
Explore
Downloads
Reports
Developer Pricing
Enterprise Access
Contact Us
My Account
Exploits
Maps
No results found

Shodan

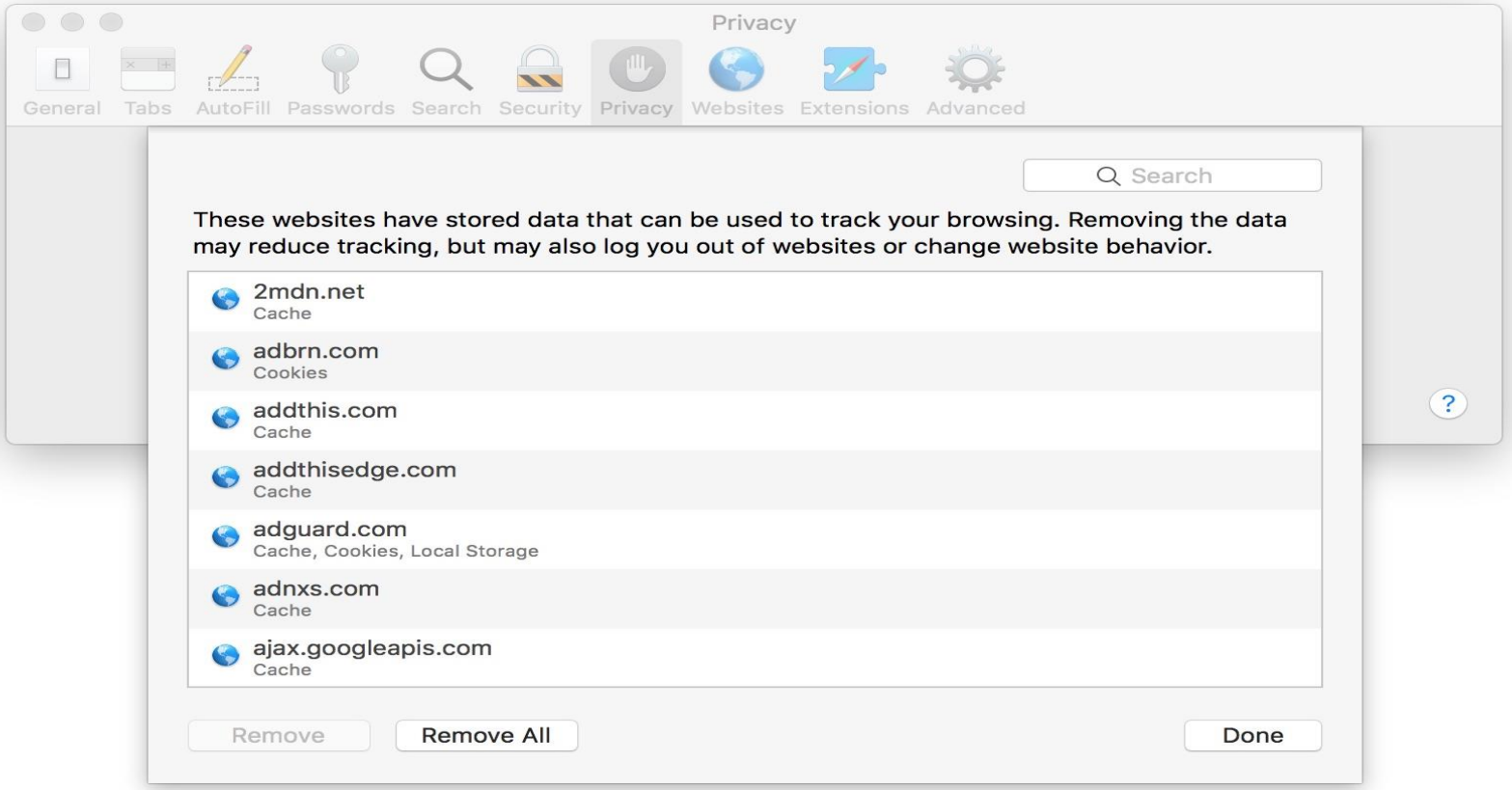
MacOS

- Update OS, Apps, settings
- Inventory
- Administrator account(s)
- Settings & Privacy
  - Allow apps downloaded from: App Store
  - Turn on Firewall
  - Disable automatic login
  - Enable FileVault
  - Location Services

Safari

- General
  Open “safe” files after download Off
- Autofill Off
- Security Enable JavaScript off
- Privacy – Prevent cross-site tracking
  Ask websites not to track me
- Extensions - to suit
- Advanced Show full website address
- Private Window (Shift command N)

- Manage Website Data button



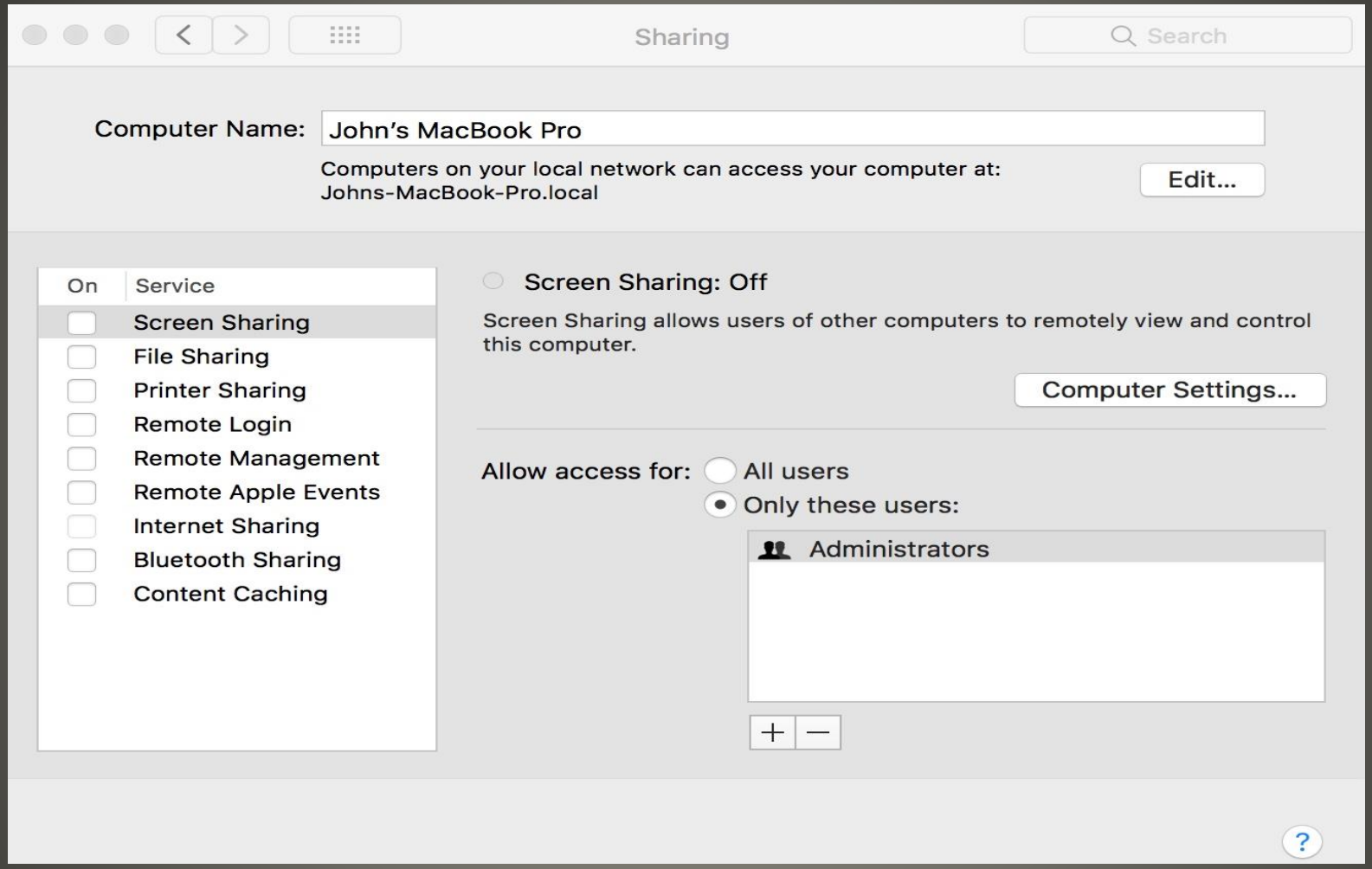
Safari Privacy

- Similar to WEB analytics but for apps
- ANY event the developer chooses

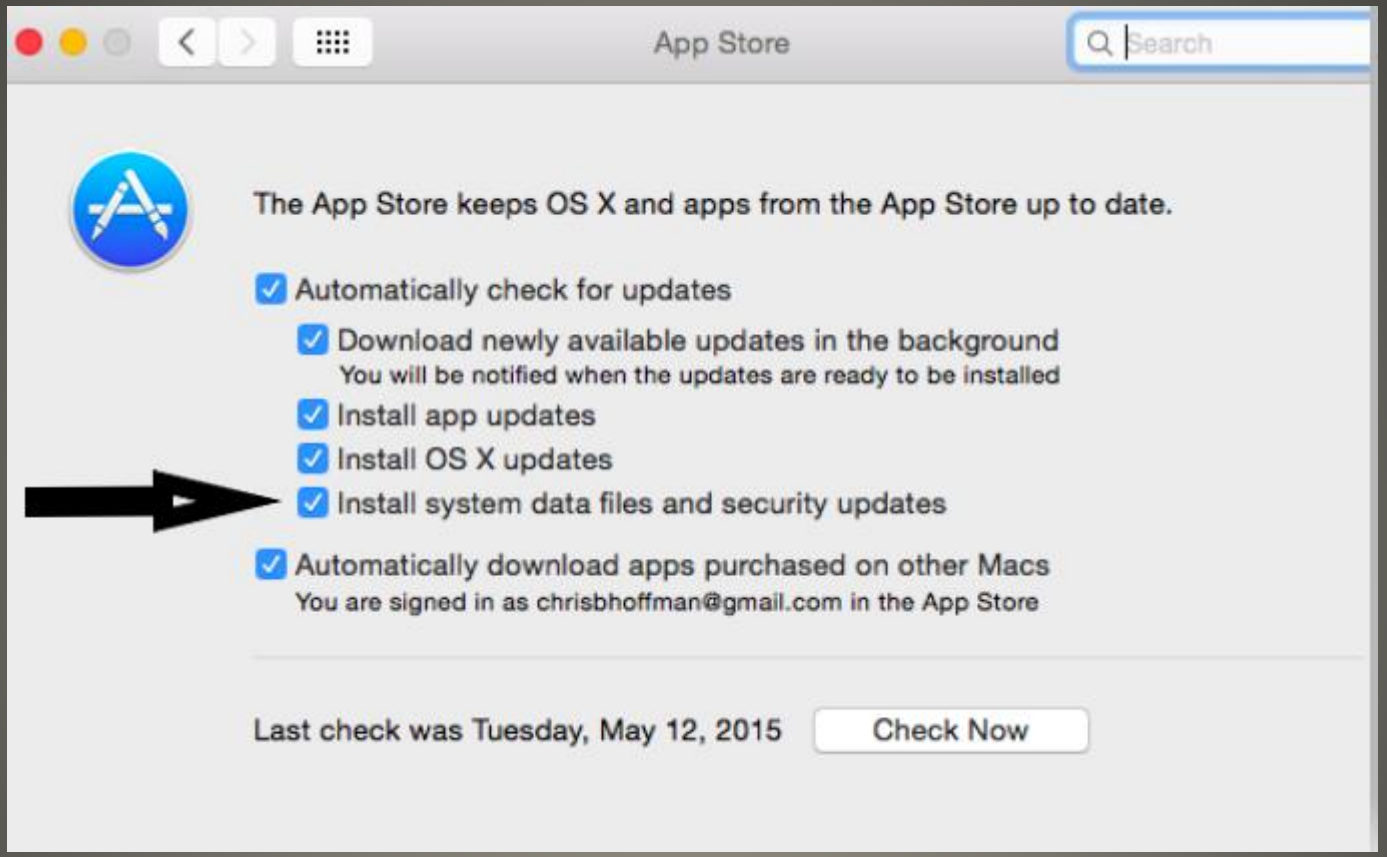
MacOS Analytics

MacOS

- KnockKnock
- BlockBlock
- Xprotect
- Bitdfender Virus Scanner
- Malwarebytes



MacOS Sharing


App Store
Search
The App Store keeps OS X and apps from the App Store up to date.
Automatically check for updates
Download newly available updates in the background
You will be notified when the updates are ready to be installed
Install app updates
Install OS X updates
Install system data files and security updates
Automatically download apps purchased on other Macs
You are signed in as chrisbhoffman@gmail.com in the App Store
Last check was Tuesday, May 12, 2015
Check Now

Xprotect

- Questions, suggestions, comments?
- The**amnesic**incognito**live**system - tails

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer

SCCCCyber@gmail.com