



WSSFC 2022

Technology Track – Session 3

Best Practices in Cybersecurity

Aaron Brooks

About the Presenter...

Aaron Brooks, Brooks Law and Consulting LLC, Naperville, IL.

BASIC COMPUTER SECURITY CHECKLIST

Aaron W. Brooks

awb@brooksfirm.law

Version 220819.1

Protection From Remote Attacks

- ☐ **Updates:** Operating system and business software are supported, patched, and set for automatic download of updates.
 - ☐ Windows clients should be Windows 10 or above (Windows 8.1 security support ends January 10, 2023).
 - ☐ Perform regular browser security checks. Consider deleting cookies regularly, or use guest browsing on non-subscription sites.
 - ☐ Keep a checklist of software, integrations, and extensions for updates.
- ☐ **Passwords:** Use a different password for each cloud-based account. Consider using a password manager to randomly generate and store secure passwords for all your accounts.
 - ☐ Consider strong passwords (more than 12 characters, randomly generated, with four degrees of complexity).
 - ☐ Consider periodically changing all passwords.
- ☐ **Multi-Factor Authentication.** Enabled MFA for all online accounts.
 - ☐ Prefer authenticator apps over text or email codes.
 - ☐ Ensure that all accounts have backup access methods (such as one-time codes or alternate addresses to receive MFA codes). Regularly test your ability to regain access to MFA-protected accounts without use of your mobile phone.
- ☐ **Phishing.** Know the difference between a proper login request and a fake login request (*particularly* with key accounts such as Google, Microsoft, and your phone/fax system).
 - ☐ Don't interact with your accounts via email.
 - ☐ Staff must be regularly trained to prevent phishing attacks.
 - ☐ Wire transfer policies require both written and verbal confirmation of routing information and all changes to transfer instructions.
- ☐ **Audit Accounts.** All online accounts are listed in a central system and reviewed regularly for fraudulent activity; passwords are changed at least every six months.

- AntiVirus Protection. Virus protection software installed on all devices, and confirmation of the following:
 - Virus definitions downloaded daily;
 - Quick scans run daily; deep scans run weekly;
 - Scan logs reviewed weekly; and
 - Protection set to scan all file openings, including email attachments and web links.
- Encryption in Transit. All data transmission mechanisms are encrypted using the most current version of each encryption protocol.¹ For example, encrypt email between your server and all devices. Use the most current and fully-updated version of web browsers and confirm that browser connections to cloud services use HTTPS. Avoid public internet services unless connected through a private and secure VPN.
 - When sending documents to others, prefer authentication-based portals (like a Microsoft Team where the recipient is a designated external user).
 - Some email systems support encryption in transit. For example, if sender and recipient are both using Gmail or MS365, then it's likely the communications are encrypted in transit.
 - Local encryption of attachments is no longer recommended (i.e. setting a password on an Adobe PDF document and then attaching it an unencrypted email). Modern cloud systems like Microsoft Teams and Dropbox have made this method obsolete.
 - When emailing documents, consider the sensitivity of the data using factors listed in the Illinois Personal Information Protection Act, and never send that information unencrypted.
- Firewall/Network. Networks protected by hardware firewalls; devices protected by software firewalls. Users know how to open and review firewall activity.
 - Regularly update home router firewall, and set the appliance to highest level of security.
 - Regularly update devices on home network. Consider separating IoT and other non-business devices on your home network.

¹ Valid encryption processes for data transmission are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

- ☐ Secure Configuration. All computing devices are set up and configured in accordance with a written configuration management policy. At a minimum, this policy should require each device to be fully encrypted and its administrative rights disabled for normal daily use.
- ☐ Cloud Services. Cloud providers have appropriate security credentials, current security risk assessments, and written security representations. An ideal security credential is the ISO 27001 certification, but other security credentials may be acceptable. Retain copies of these documents for seven years, or such other document retention laws and policies that may be applicable.
 - ☐ Cloud services should be contracted under business-level terms and conditions. Consumer level terms are not sufficient.
 - ☐ Cloud services contracts meet standards in ISBA Advisory Opinion No. 16-06.

Protection From Local Attacks

- ☐ Encryption at Rest. All storage devices are encrypted in accordance with NIST Special Publication 800-111. Examples to remember:
 - ☐ Desktop and laptop hard drives
 - ☐ External storage drives
 - ☐ Mobile phones and iPads
 - ☐ Flash or Thumb drives
 - ☐ CDs or DVDs containing confidential information
- ☐ End of Life. All storage devices are destroyed at end of life.
 - ☐ Record device serial number and date of destruction in technology records and retain for six years.
 - ☐ Contracts for leased equipment provide for secure deletion of data if the equipment is storage-enabled.
- ☐ Consider Social Engineering and Other On-Prem or On-Device Threats. Do not let unauthorized people or devices interact with your systems.
 - ☐ Don't accept third-party or unknown USB devices
 - ☐ Keep server equipment locked and supervised
 - ☐ As for identification and presume cold callers guilty until proven innocent
- ☐ Wireless Networks. Wireless networks are encrypted, and default admin passwords are changed.

Best Practices in Cybersecurity

Aaron W. Brooks
awb@brooksfirm.law

Brooks Law and Consulting, LLC
Naperville, IL

```
error_mod = modifier_ob
mirror object to mirror
error_mod.mirror_object =
operation == "MIRROR_X":
error_mod.use_x = True
error_mod.use_y = False
error_mod.use_z = False
operation == "MIRROR_Y":
error_mod.use_x = False
error_mod.use_y = True
error_mod.use_z = False
operation == "MIRROR_Z":
error_mod.use_x = False
error_mod.use_y = False
error_mod.use_z = True

selection at the end -add
ob.select= 1
r_ob.select=1
text.scene.objects.active
"Selected" + str(modifier
error_ob.select = 0
bpy.context.selected_ob
to.objects[one.name].se

int("please select exact

-- OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ect.mirror_mirror_X"
for X"

context):
text.active_object is not
```

Develop a Framework Mentality

- See the included Basic Computer Security Checklist
- Read *NIST Small Business Information Security: The Fundamentals*
- Understand the basic purpose of information security frameworks, like the NIST Cybersecurity Framework.

Understand
the Nature of
Various Attack
Surfaces

Avoid Exploit Wednesday

Calendar Patch Tuesday

AWB

Key Updates

- Device Firmware
- Windows
- Office/Teams/Adobe
- Chrome/Firefox
- Mobile Devices
- IoT

Password Management Rules

In Order of Importance

- Use a different password for every account
- Make each password long and random
- Include 4 degrees of complexity (Number, Uppercase, Lowercase, Symbol)
- Periodically change all your passwords

HOW LONG WILL IT TAKE TO CRACK YOUR PASSWORD

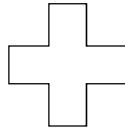
number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Create Your Own Language for Key Accounts

#U\$3@N3w\$B00z37Ch3wz^

Practice with Flashcards Weekly

ViqaS#2#-H@bR4k7F-ed



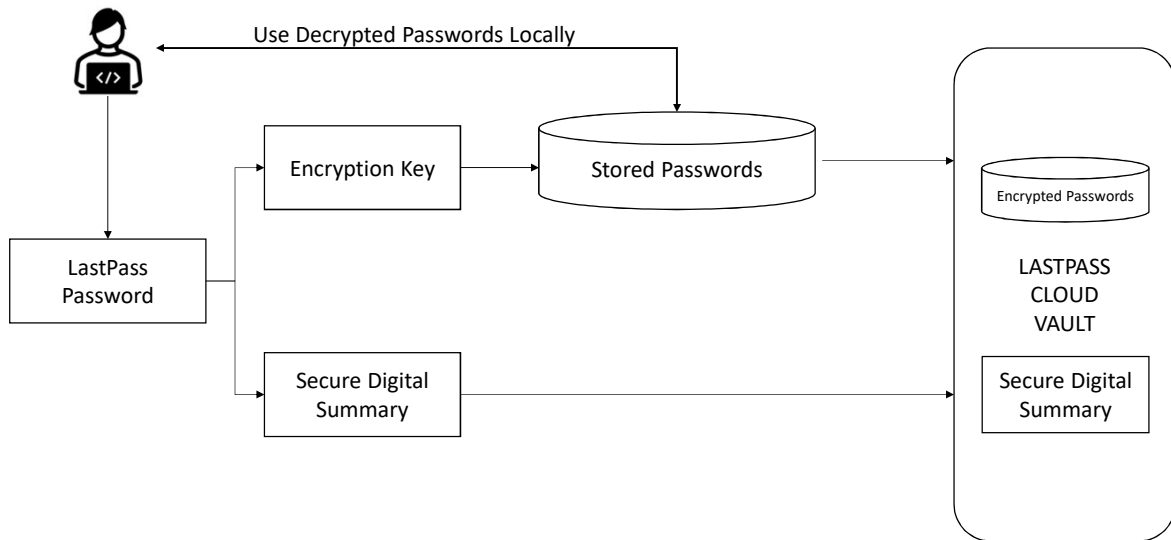
LastPass...

AWB

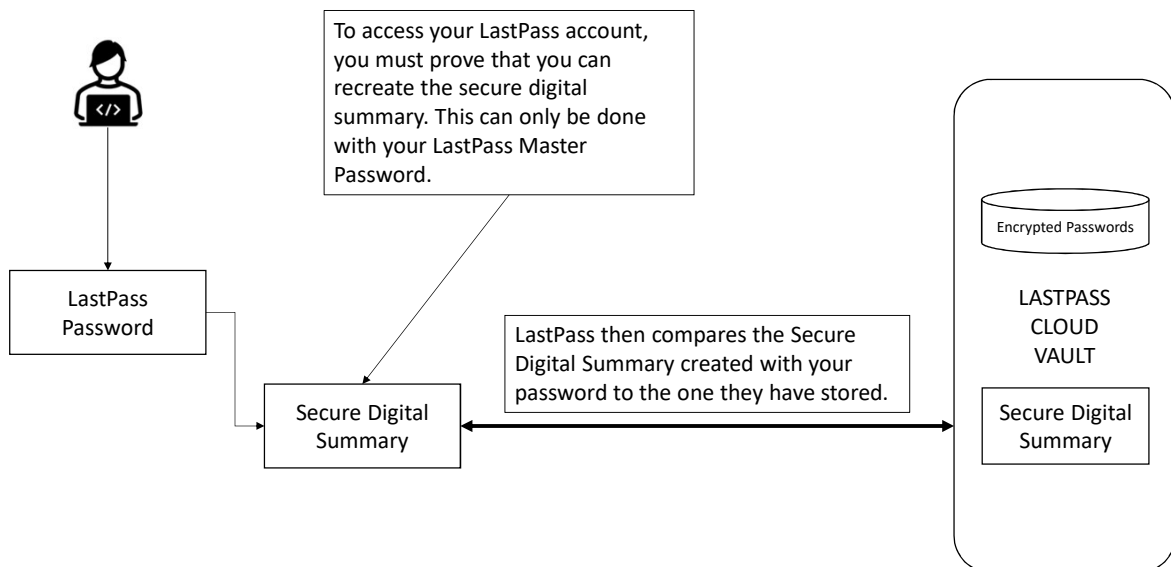
The screenshot shows the LastPass password generator interface. At the top, there is a 'Back' button. Below it, a password is displayed: 'V8^26YVYK%\$w15BNqsh%DcNR'. To the right of the password are icons for copying and refreshing. Below the password is a 'SHOW HISTORY' link. Underneath, there are settings for 'Password length' (set to 24) and three radio button options: 'Easy to say', 'Easy to read', and 'All characters' (which is selected). To the right of these are four checked checkboxes: 'Uppercase', 'Lowercase', 'Numbers', and 'Symbols'. At the bottom right, there is a 'FILL PASSWORD' button.

Always use this
tool when you
need to create
a password

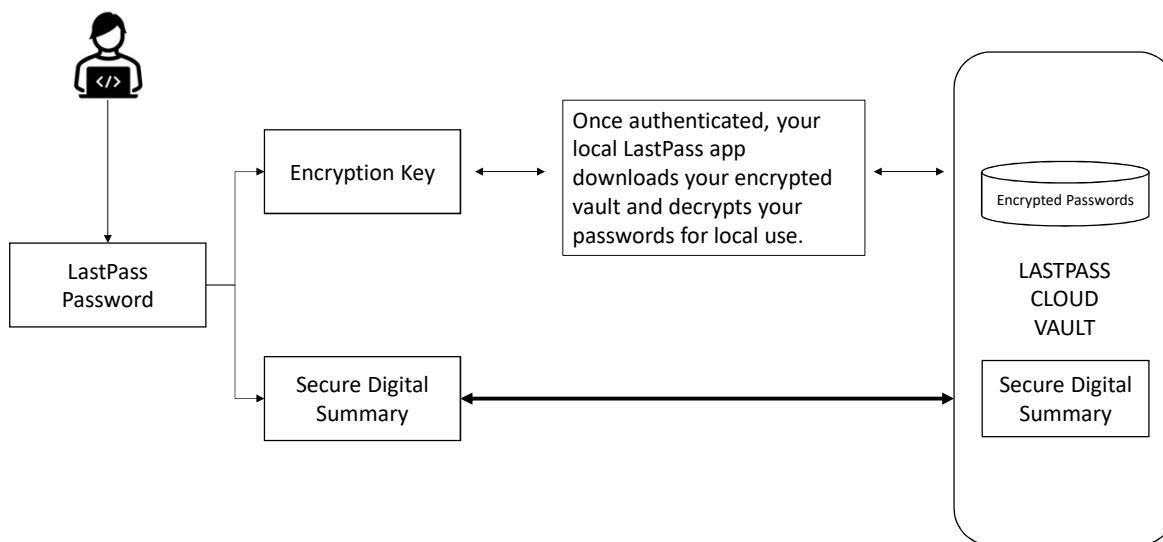
LastPass Does Not Store Your Password or Unencrypted Vault



Log In By Proving You Know Your LastPass Master Password



Download Your Encrypted Vault and Use Passwords Locally



Key MFA Tools



Authenticator applications



Text to a device



Email to an unconnected service



Printed backup codes

Consistently Test MFA Backup Methods

Approve sign in request



Open your Microsoft Authenticator app and approve the request to sign in.

I can't use my Microsoft Authenticator app right now

More information

Regularly think through your back-up plan.

Unique Usernames

The Next
Level of
Secure



Register a domain name



Create an email account with "catch-all" privileges



Create unique email addresses for each new account

Don't Open
Accounts
from Email

Google is hiring: Associate Product Counsel, Chrome.



LinkedIn <jobs-listings@linkedin.com>
To: Aaron Brooks

Reply Reply All Forward

Mon 6/6/2022 4

If there are problems with how this message is displayed, click here to view it in a web browser.



Top job picks for you



Associate Product Counsel, Chrome

Google · Chicago, Illinois, United States

Be one of the first 14 applicants



Associate General Counsel Sr. - Digital Platforms - NEW

Anthem, Inc. · Chicago, Illinois, United States

Be the first applicant to apply

Associate General Counsel - Digital Platforms - NEW

Don't Reset
Accounts
from Email

Re: Re: Password Expiry Notification 86710



Credentials <miguel.rodriguez@gamas.com.mx>
To: Aaron Brooks

This message was sent with High importance.

WARNING: This email originated outside of HolmstromKennedy.

DO NOT CLICK links or attachments unless you recognize the sender and know the content

OFFICE-365

The password for your email (abrooks@holmstromlaw.com) expires today, you should keep your password

[Keep My Current Password](#)

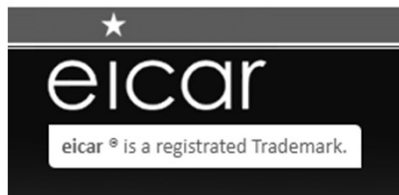
Use Virus
Protection
Software Properly



AWB

EUROPEAN EXPERT GROUP FOR IT-SECURITY


DOWNLOAD
ANTI MALWARE TESTFILE



test

INSTALL A VIRUS ON YOUR
COMPUTER

AWB



Use and Understand Encryption

- Data at Rest
- Data in Motion

AWB


> Control Panel > System and Security > BitLocker Drive Encryption

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker on



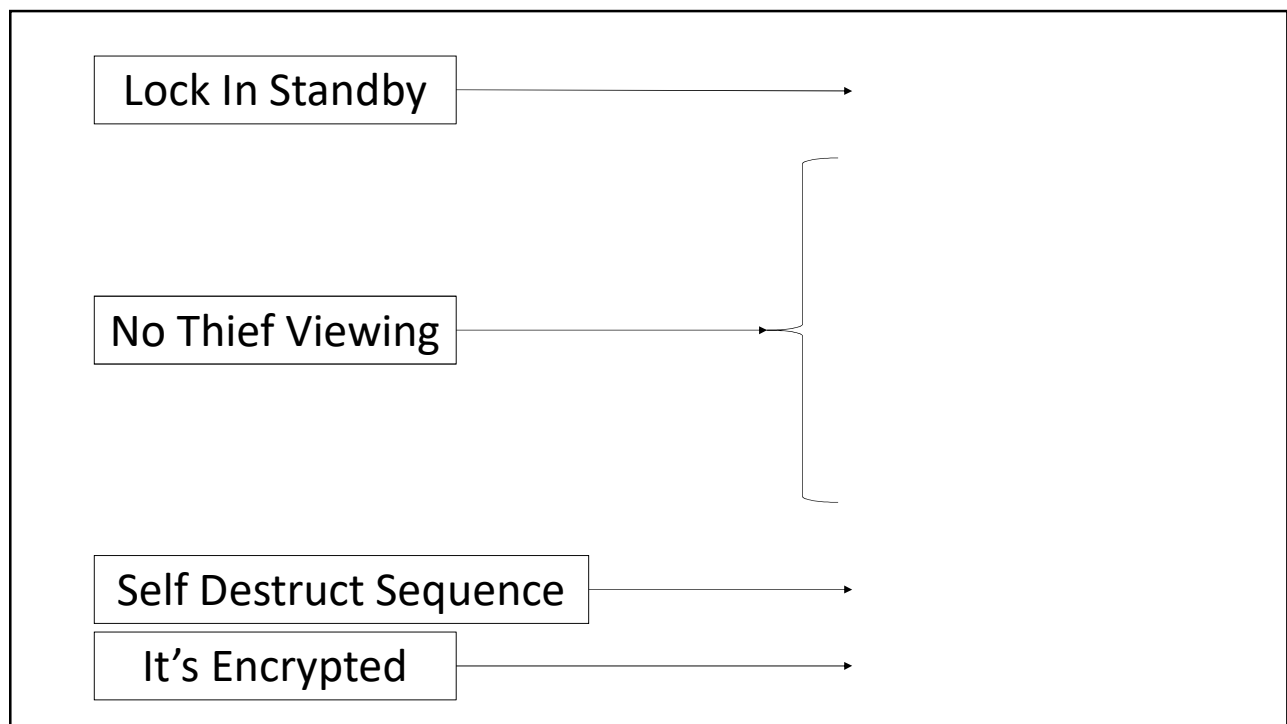
Suspend protection

Change how drive is unlocked at startup

Back up your recovery key

Turn off BitLocker

Fixed data drives



ISBA Professional Conduct Advisory Opinion No. 96-10

Lawyers may use unencrypted email without
client authorization

(however)

New IRPC 1.6 requires “reasonable” efforts to
protect client confidentiality

Okay to Send Encrypted PDF Attachments?

First, the file isn't protected from brute force attacks. Thus, password must be sufficiently complex to withstand attacks.

Second, the file can be perpetually stored for future technology attacks.

Third, the password must be securely transferred (not sent in a second unencrypted email).

Provide a secure download using ShareFile, DropBox, Box, NetDocuments or other secure file transfer method.

Be very careful with public Wi-Fi services

AWB

Beware of Commercial VPN Services

- The VPN provider can see, log and even modify all your internet traffic
- Improperly configured VPN can give others direct access to your local network
- Improperly configured VPN can allow data leakage, thereby defeating the purpose



ShieldsUP!!tm

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Determine the status of your
system's first 1056 ports

FAILED

**TruStealth
Analysis**

FAILED

Firewall Security Level

☐ Maximum Security (High)

☐ Typical Security (Medium)

☒ Minimum Security (Low)

LAN-to-WAN : Allow all.

WAN-to-LAN : Block as per below and enable IDS.

IDENT (port 113)

☐ Custom Security

SAVE SETTINGS

RESTORE DEFAULT SETTINGS

PASSED

TruStealth
Analysis

PASSED

Firewall Security Level

☐ Maximum Security (High)

☒ Typical Security (Medium)

LAN-to-WAN : Allow all.
WAN-to-LAN : Block as per below and enable IDS.
IDENT (port 113)
ICMP request
Peer-to-peer apps:
kazaa - (TCP/UDP port 1214)
bittorrent - (TCP port 6881-6999)
gnutella- (TCP/UDP port 6346)
vuze - (TCP port 49152-65534)

☐ Minimum Security (Low)

☐ Custom Security

SAVE SETTINGS

RESTORE DEFAULT SETTINGS

PASSED

TruStealth
Analysis

PASSED

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Maintain a Device Configuration Policy

- Factory reset new devices
- Remove preinstalled adware, if any
- Apply and confirm all firmware, OS and application updates
- Apply and confirm encryption
- Apply and confirm endpoint management policies



RESET YOUR PHONE AND COMPUTER

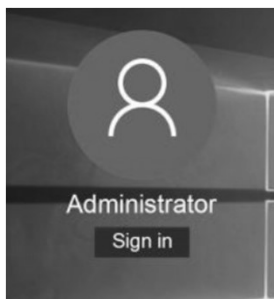
Live with a factory
reset mentality

AWB

Destroy Old Hard Drives



AWB

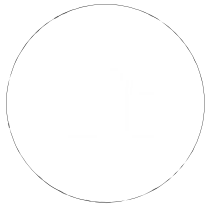


**Disable administrative rights
on your computer**

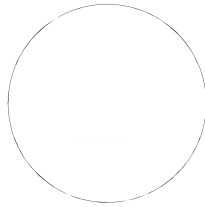
**Administrative mode gives
hackers and viruses
unrestricted access to
computer**

AWB

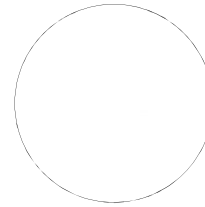
USB Devices Are Risky



MALWARE FILES



AUTORUN FILES



EMBEDDED MALWARE

AWB

Again: Develop a Framework Mentality

- See the included Basic Computer Security Checklist
- Read *NIST Small Business Information Security: The Fundamentals*
- Understand the basic purpose of information security frameworks, like the NIST Cybersecurity Framework.