U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Cybersecurity 101

Ian Moore, CISSP
Cybersecurity State Coordinator (CSC) for Washington State
Cybersecurity Advisor (CSA) Program
Cybersecurity and Infrastructure Security Agency

Challenge - Rules of Engagement

I’ve placed common electrolytes throughout this presentation.

Count them all and write the total on the back of your business card and take that to the CISA booth and get a prize.

- Only 1 prize per person, the first 20 get a prize

Contents

- Shields Up!
- Cybersecurity Basics
- Passwords - One Level Deeper
- Staying Safe Online
- Social Engineering and Phishing
- Mitigate Effects of Malware & Ransomware
- Malware & Ransomware Response Procedures
- Quick Response (QR) Codes

Fear, Uncertainty, and Doubt

Increase your awareness
of cybersecurity

SHIELDS UP

Latest Updates

- Sharing Cyber Event Information: Observe, Act, Report
- CISA/DOE Insights: Mitigating Attacks Against **Uninterruptible Power Supply** Devices
- **Tactics, Techniques, and Procedures** of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- Statement by President Biden on our Nation's Cybersecurity
- White House Fact Sheet: **Act Now to Protect Against Potential Cyberattacks**
- Strengthening Cybersecurity of **SATCOM** Network Providers and Customers
- Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting **Default Multifactor Authentication** Protocols and 'PrintNightmare' Vulnerability
- Updated: Conti Ransomware Cybersecurity Advisory
- Shields Up Technical Guidance
- **UPDATED 19 April: Known Exploited Vulnerabilities Catalog**

https://www.cisa.gov/shields-up

- **CVE-2018-6882**
  - Zimbra - Collaboration Suite (ZCS) Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability
  - 2022-04-19
    - Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability that might allow remote attackers to inject arbitrary web script or HTML. Apply updates per vendor instructions.

- **CVE-2019-3568**
  - Meta Platforms – WhatsApp - WhatsApp VOIP Stack Buffer Overflow Vulnerability
  - 2022-04-19
    - A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. Apply updates per vendor instruction

- **CVE-2022-22718**
  - Microsoft – Windows - Microsoft Windows Print Spooler Privilege Escalation Vulnerability
  - 2022-04-19
    - Microsoft Windows Print Spooler contains an unspecified vulnerability which allow for privilege escalation. Apply updates per vendor instructions.

https://www.cisa.gov/shields-up

SHIELDS UP

SHIELDS UP Guidance for All Organizations

- **Reduce the likelihood of a damaging cyber intrusion**
  - Remote Access
  - Update Software
  - Disable Ports and Protocols
  - Strong Cloud Controls
- **Take steps to quickly detect a potential intrusion**
  - Notice Unusual Behavior
  - AV/AM Software Sigs Updated
  - Monitor and Inspect Traffic - Ukraine
- **Ensure that the organization is prepared to respond if an intrusion occurs**
  - Quality IR Team
  - Key Personnel – Surge Support
  - IR TTX - Roles
- **Maximize the organization's resilience to a destructive cyber incident**
  - Test Backups
  - Test Manual Controls in ICS/OT env.

https://www.cisa.gov/shields-up

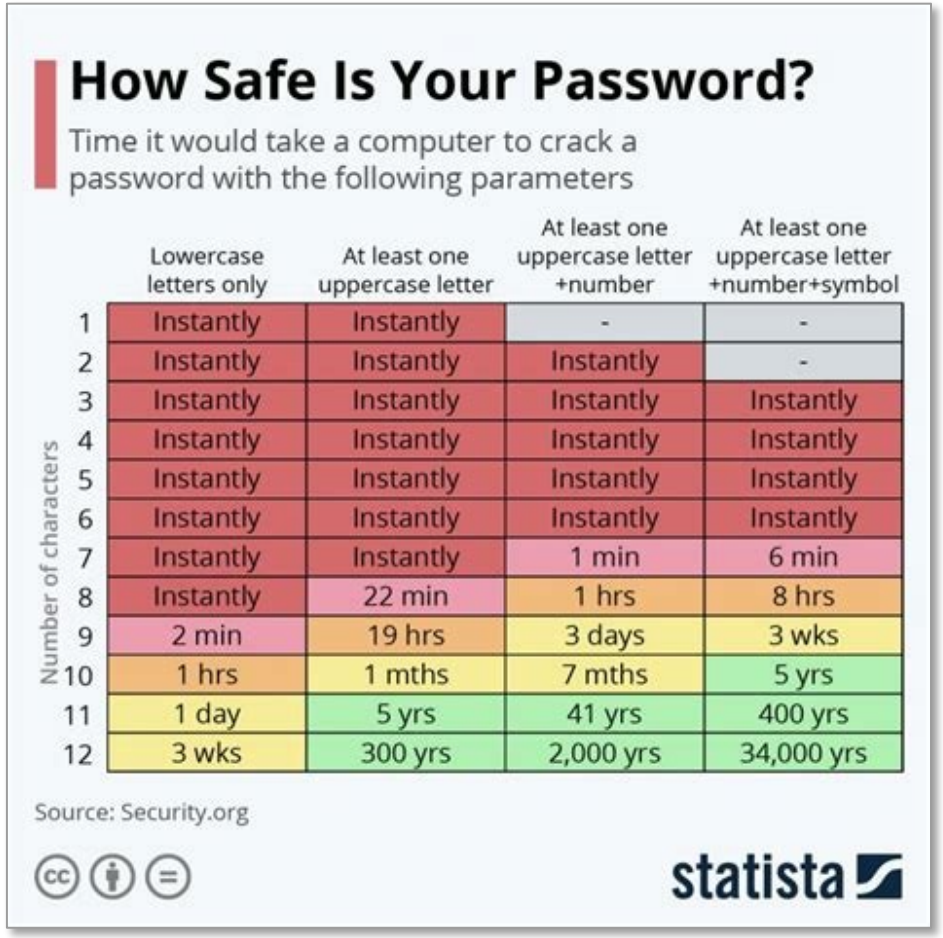
Cybersecurity Basics

- Anti-virus/malware (AV/AM) software
- Passwords
  - Storage
- Account security
  - Security Settings
- Mobile devices and work networks
  - Knowing what and how to connect
  - Charging
  - AV/AM software
- Bluetooth security
- Wireless security
  - When to trust a network
  - VPNs
- USB devices
  - Don’t connect unless you know for certain what’s on it

Passwords - One Level Deeper

- Complexity requirements
  - (Upper, lower, #, special char)
- Length Requirements
  - 10 characters minimum is best practice
- Password Age
  - Based on time to crack
- Password Reuse – don't allow
- Password Patterns – minimize or could be guessable
- Using the same password for multiple systems/sites

Brute Force, not Rainbow Tables



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

Sample Passwords:
hello, hellothere, HelloThere, H3lloTher3, H3!!o_Ther3

Staying Safe Online

- Social Media Concerns
- Privacy Concerns
- Online Personas
- Trust No One Online!
- Passwords
- Usage Rules

calcium

AI/ML

Stand on soap box here!

Social Engineering and Phishing

- Social Engineering
  - Establishing **rapport**
  - Making some connection
  - **Smiling** and acting friendly
  - Opportunity to help out
  - May be multiple interactions
  - **Goal: To get information from you that you wouldn't normally give out**
- Phishing
  - Email trying to get you to click it
  - May be from someone **you may know**
  - The domains will be different
  - Some **urgency** to act
  - Link or attachment
  - Frequently **target leadership** that may be less technical

Mitigate Effects of Malware & Ransomware

- Implement baseline cybersecurity controls
- Backup, backup, backup
- Don’t click on links and attachments from people you don’t know
  - Even if you know the sender, ask, “Does this attachment or link seem normal from this person?”
- Don’t surf to sites that you don’t know
  - Search Engine Poisoning

Malware & Ransomware Response Procedures

magnesium

- Malware & Ransomware in your office
  - Disconnect system from network if wired connection
  - If wirelessly connected, IT Support will kick you off network, if they can
  - Leave powered on, if you can
    - RAM scraping – forensic evidence
      - Encryption keys, user accounts, malware evidence, IP addresses, etc.
  - Call IT Support for guidance

Quick Response (QR) Codes

- QR Code Security and Risk
  - Devices show the domain
  - May be malicious page/site inside of the safe domain
  - Know the domain you think you are going to – sanity check
  - Pay attention to sub-domains
  - Don’t trust them by default
- Hacker Anecdote – the good and the bad

Conclusion

- Shields Up!
- Cybersecurity 101
- Passwords - One Level Deeper
- Staying Safe Online
- Social Engineering and Phishing
- Mitigate Effects of Malware & Ransomware
- Malware & Ransomware Response Procedures
- Quick Response (QR) Codes

CISA Cyber Resources
https://www.cisa.gov/cyber-resource-hub

Region 10 Cybersecurity Contacts and Questions?

Chris Callahan
Chief, Cybersecurity (CCS)
(202) 702-6706
CHRISTOPHER.CALLAHAN@cisa.dhs.gov

Theresa Masse
CSC for Oregon
503-930-5671
theresa.masse@cisa.dhs.gov

Josh Stemp
CSC for Idaho
208-761-9882
joshua.stemp@cisa.dhs.gov

Ron Watters, GSLC
Region 10 (WA, OR, ID, AK)
Cybersecurity Advisor
(206) 348-4071
Ronald.Watters@cisa.dhs.gov

Mark Breunig
CSC for Alaska
907-795-5673
mark.breunig@cisa.dhs.gov

Ian Moore
CSC for Washington
(360) 594-1832
Ian.Moore@cisa.dhs.gov

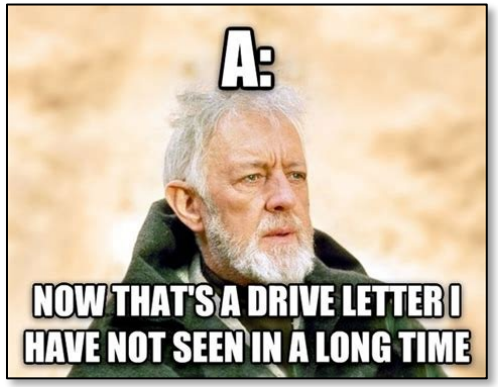
Contact CISA (via the reporting portal or by phone at 1-888-282-0870) to report an intrusion or to request either technical assistance or additional resources for incident response.
CyberLiaison@cisa.dhs.gov

For inquiries or further information, contact cyberadvisor@cisa.dhs.gov

phosphate

Meme Break

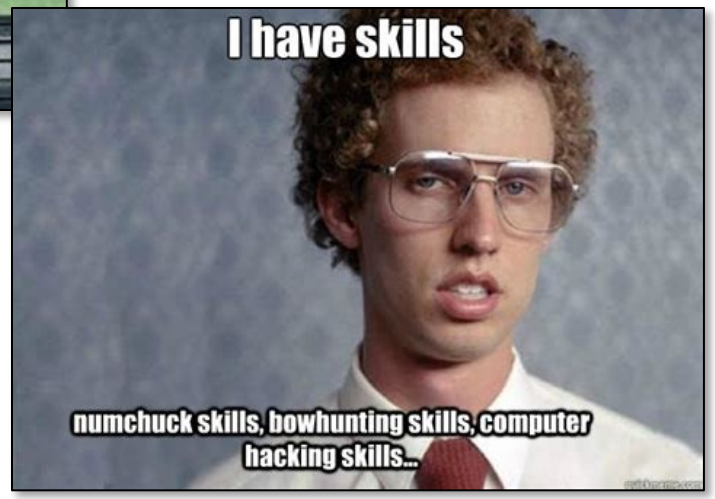

WITH THE LOCKDOWN YOU WILL HAVE SOME TIME TO REST
I WORK IN CYBERSECURITY


A:
NOW THAT'S A DRIVE LETTER I HAVE NOT SEEN IN A LONG TIME


Application: *Not responding*
Me:
MORE MEMES FOR PROGRAMMERS
@programer.life
Task Manager


WHEN YOU OPEN UP YOUR FRIENDS COMPUTER AND THEY ARE ALREADY LOGGED INTO FACEBOOK
HACKERMAN


" BACKUPS " ?!
...WHAT'S "BACKUPS" ?!
So, tell me about your backups.


I have skills
numchuck skills, bowhunting skills, computer hacking skills...


WITH THIS TECHNOLOGY
WE WILL BRING THE UNITED STATES TO ITS KNEES


MY COWORKERS THINK I'M A HACKER
BECAUSE I KEEP THE COMMAND PROMPT OPEN ON MY MONITOR