Welcome to today's University Business web seminar

Security without Barriers: Enabling Secure Remote Access for Your Campus

Kurt Eisele-Dyrli
Web Seminar Editor
University Business

Randy Marchany
University IT Security Officer
Virginia Tech

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

Thank you for joining us!
The web seminar will start promptly at 2:00 ET.

UB University Business

FIREEYE

Welcome to today's University Business web seminar

Security without Barriers: Enabling Secure Remote Access for Your Campus

Thank you for joining us!
The web seminar will start shortly at 2:00 ET.

For technical support:
Use the Chat panel at the right of your screen. Select the name of our event producer, Jason York, and type your message.

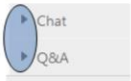
"Chat" for tech support

No computer speakers? Prefer to listen privately?
Dial the phone number and access code posted in the Chat window.

To submit a question to our panel:
Use the Q&A panel at the right of your screen. Send your question to All Panelists, the default option.

"Q&A" for panelist questions

Don't see a panel?
Click the "expand panel" triangle in front of the panel name.



Need to access the presentation at a later time?
Everyone will receive an email with links to the slides and the archive recording.

UB University Business

FIREEYE

Welcome to today's University Business web seminar

Security without Barriers: Enabling Secure Remote Access for Your Campus

Kurt Eisele-Dyrli
Web Seminar Editor
University Business

Randy Marchany
University IT Security Officer
Virginia Tech

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

UB University Business

FIREEYE

Welcome to today's University Business web seminar

This web seminar is sponsored by:

Welcome to today's University Business web seminar

Security without Barriers: Enabling Secure Remote Access for Your Campus

Kurt Eisele-Dyrli
Web Seminar Editor
University Business

Randy Marchany
University IT Security Officer
Virginia Tech

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

UB University Business

FIREEYE

Housekeeping

Security without Barriers: Enabling Secure Remote Access for Your Campus

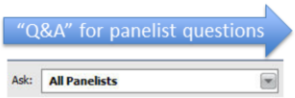
For technical support:
Use the Chat panel at the right of your screen. Select the name of our event producer, Jason York, and type your message.

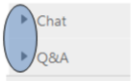
No computer speakers? Prefer to listen privately?
Dial the phone number and access code posted in the Chat window.

To submit a question to our panel:
Use the Q&A panel at the right of your screen. Send your question to All Panelists, the default option.

Don't see a panel?
Click the "expand panel" triangle in front of the panel name.

Need to access the presentation at a later time?
Everyone will receive an email with links to the slides and the archive recording.





Welcome to today's University Business web seminar

Security without Barriers: Enabling Secure Remote Access for Your Campus

Kurt Eisele-Dyrli
Web Seminar Editor
University Business

Randy Marchany
University IT Security Officer
Virginia Tech

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

UB University Business

FIREEYE

FIREEYE™

Security Without Barriers

Enabling Secure Remote Access for Your Campus

Christian Schreiber, CISM, PMP
Cybersecurity Platform Strategist – FireEye

Personal Background

20+ years IT and security experience

- Security leadership: The University of Arizona, University of Wisconsin – Whitewater, SunGard Data Systems / Ellucian
- IT leadership positions: University of Wisconsin – Madison, Central Michigan University

Education and Certifications

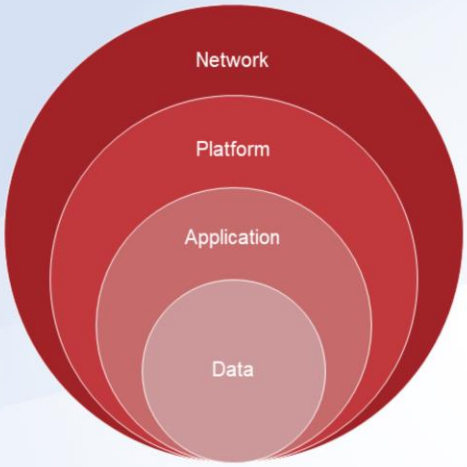
- Bachelor of Science in Business Administration from Central Michigan University
- Masters Certificate in Project Management from University of Wisconsin – Madison
- Certified Information Security Manager (CISM)
- Project Management Professional (PMP)

- **Joined FireEye in 2016**
  - Strategist helping customer executives achieve effective and resilient cybersecurity
  - Focus on education, healthcare, and public sector customers

Exploring security concepts

How do you describe your cybersecurity strategy?

Strategies often described as “defense-in-depth”



What do these analogies have in common?

They describe methods of **PREVENTING** attackers from reaching your assets

Asymmetric threats

- No technical solution can prevent all attacks all the time
- There will always be bad actors looking to exploit that security gap

Change the narrative about your security goals: Castle vs Museum

- **Museums must protect valuable assets**
  - while creating an open welcoming environment
  - and allowing visitors within inches of the assets

Underlying goals are different

Castle Analogy	Museum Analogy
• GOAL: Protect assets by **preventing** attackers from gaining entry	• GOAL: Protect assets while **enabling** visitors to gain entry

- A museum cannot be successful if visitors have a hard time gaining access

Key assets treated differently

Castle Analogy	Museum Analogy
• GOAL: Valuable assets are **isolated** making them difficult for attackers to reach	• GOAL: Valuable assets are **highlighted** making them easier for visitors to reach

- Visitors are encouraged to visit the most important assets in a museum

Monitoring approached differently

Castle Analogy	Museum Analogy
• GOAL: Cover the **perimeter** thoroughly • Focus on preventing bad actors from **gaining access**	• GOAL: Cover the **interior** thoroughly • Focus on preventing bad actors from **exploiting access**

- **Museums must assume bad actors can act from inside the perimeter**

Building a cyber resilience strategy

Applying lessons learned from a museum

What do we mean by "cyber resilience"?

Prevent Incidents

- Identify threats early to help prevent a security incident

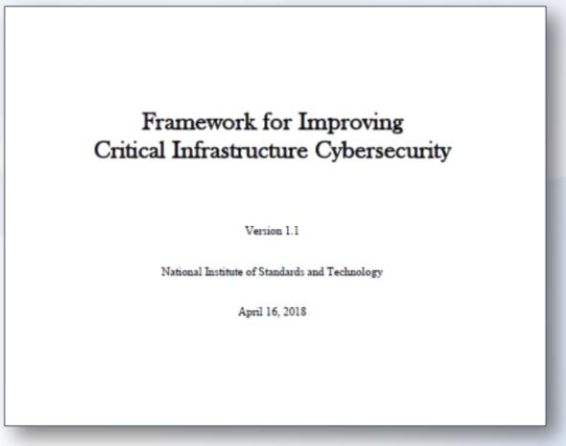
Reduce Impact

- Disrupt the attack chain and act to mitigate damage

Improve Efficiencies

- Make better use of your resources

Using the NIST Cybersecurity Framework (CSF) to design a resiliency strategy



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

How does a museum approach breach resilience?

* Accessed online from http://www.montel.com/en/markets/museum-mobile-shelving-storage/museums

Identify

- Maintain accurate inventory
- Identify visitors (tickets / passes)
- Employee background checks

Protect

Detect

Respond

Recover

Maintain inventory of data assets

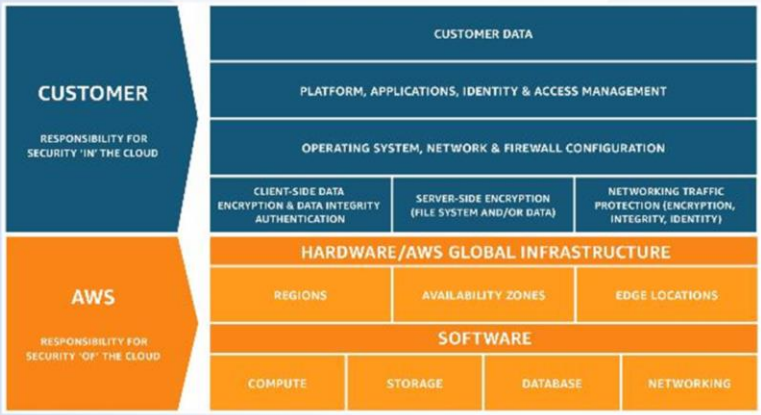
- **"If we guard our toothbrushes and diamonds with equal zeal, we'll lose fewer toothbrushes and more diamonds."**

  – McGeorge Bundy

Understand your regulations

- Map data assets to regulations
- Map regulations to your security framework
- Don't let new regulations distract from your strategy

Understand your cloud security responsibilities



* Amazon AWS. "Shared Responsibility Model." Available online at https://aws.amazon.com/compliance/shared-responsibility-model/

- "Security and Compliance is a shared responsibility between AWS and the customer…"*
- Providers help secure underlying components, but you are ultimately responsible for securing your data.

How does a museum approach breach resilience?

* Accessed online from https://www.louvre.fr/en/security-officer

Identify

Protect

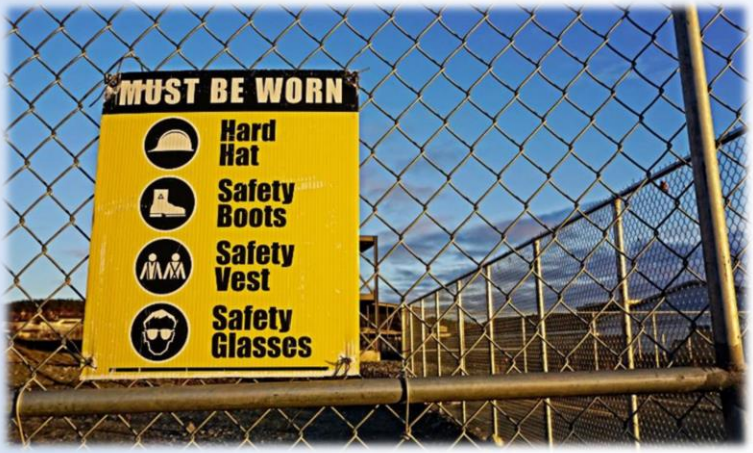
- Implement physical barriers to protect high-risk assets
- Limit visitor flow to specific entry points
- Implement additional visitor checkpoints around high-risk collections

Detect

Respond

Recover

Operationalize your security efforts



- Incorporate security into daily processes
- Cannot delegate to security team

Continuously train your stakeholders

- Require at ALL levels of the organization
- Everyone understands their role and responsibilities

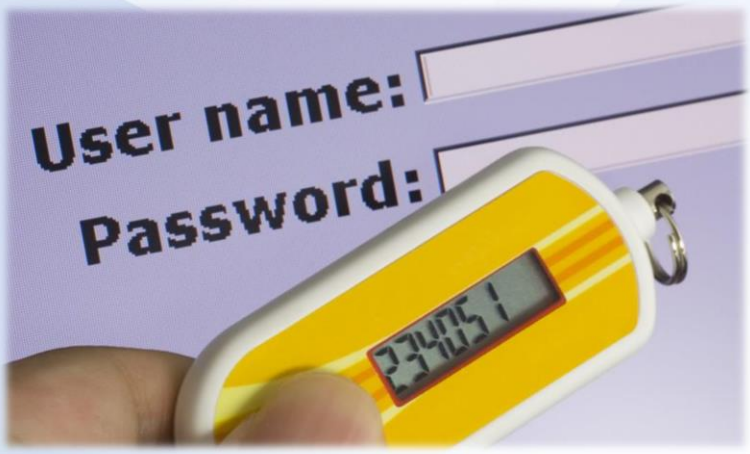
Maintain your technology with good hygiene

- Patch in a timely manner
- Use supported OS versions
- Implement comprehensive malware prevention

Strengthen your architecture

- Separate what's truly public from what should be internal
- Implement risk-based network segmentation
- Implement role-based data segregation

Strengthen your authentication



- Use multi-factor authentication
- Use credential and privilege management tools
- Authenticate DEVICES that connect to your networks

How does a museum approach breach resilience?

Identify

Protect

Detect

- Pervasive monitoring (cameras, motion sensors)
- Apply intelligence with AI, facial recognition, etc.
- Deploy guards to monitor visitor activity

Respond

Recover

Extend your visibility across the enterprise

- **Implement protection and detection tools at trust boundaries**
- **Ensure that all attack vectors have coverage**
  - Network
  - Email
  - Endpoint
  - Cloud

Consolidate your visibility

- **Avoid creating visibility silos to improve your detection capabilites**
  - Network / datacenter
  - Cloud provider
  - Authentication
  - Security tools
- **Ensure availability and integrity of logs**

How does a museum approach breach resilience?

* Accessed online from https://www.asmag.com/showpost/13890.aspx

Identify

Protect

Detect

Respond

- Empower guards to respond to threats
- On-demand protective barriers
- Fire / smoke suppression systems

Recover

Strengthen your detection and response capabilities

- Don't rely on prevention alone
- Limit attacker dwell time
- Practice regularly (e.g. table top drills)

How does a museum approach breach resilience?

* Accessed online from https://www.smithsonianmag.com/smart-news/professor-helps-bust-italian-art-theft-ring-180963563/

Identify

Protect

Detect

Respond

Recover

- Insurance
- Escalation to law enforcement
- Tracking mechanisms

Engage your leadership before a crisis occurs

- Evaluate potential value of cyber insurance
- Implement proactive incident response retainers
- Identify and train crisis response team members

Maintain your business continuity and recovery plans

* Accessed online from https://www.canada15edgedatacenters.com/good-info-on-backup-disaster-recovery/

- **Determine your risk tolerance**
  - E.g. are hot/cold standby sites needed?
- **Restore from backup when cost effective and no regulatory issues**
- **Test your backup & recovery processes, tools, and procedures**

Reporting your progress

Maintain your metrics and share with stakeholders

- Provide answers, not alerts
- Consider using third party commercial benchmarking tools

WFH! *(Work From Home!)*

Randy Marchany

CISO, Virginia Tech

VA Tech IT Security Office & Lab

Marchany@vt.edu

Twitter: @randymarchany

VIRGINIA TECH.

About Me

- **CISO**, Virginia Tech, Senior SANS Institute instructor
- Degree in Computer Science, Electrical Engineering, 3 cybersecurity patents
- Musician Indie Award Winner, wrote original theme song fo NPR program, “World Café”, toured US, Europe with the band No Strings Attached
- Former Assistant Volleyball Coach, VA Tech, USVA Club coac
- Biking (bicycle, motorcycle), volleyball

Hacker Attack Goals

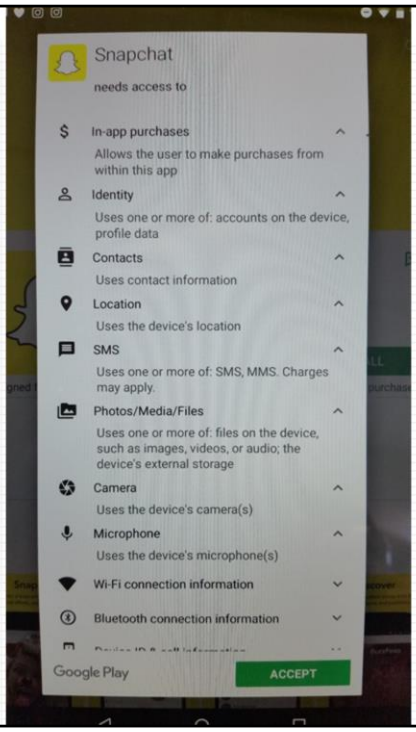
Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
- **ATTACK** other sites using hacked assets
- **DESTRUCTION** of company data (deletion or ransomware).

- **DEFEND** accordingly

VIRGINIA TECH.

https://www.sans.org/security-awareness-training/resources/posters/you-are-target



VIRGINIA TECH.

Corona & Spring Break…

- 3/8-11 Spring Break -> 3/8-3/22 extended spring break
- Office went remote week of 3/15. VT went **reduced operations** mode
- VA went Stay-At-Home 3/30/20. VT went **essential operations** mode
- ~4500 classes converted to 100% online format by ~2400 faculty
  - ~33K students taking classes
  - ~8K faculty, staff working from home

VIRGINIA TECH.

Net Access isn't Equal

- Some areas have no internet access
- Some areas have poor internet access
  - https://it.vt.edu/resources/home-internet-tips.html
- ISP rate based charge structure
- Campus WiFi Parking lots
  - https://vtnews.vt.edu/notices/it-nis-driveupwifi.html

- EDITORIAL COMMENT – My Opinion only (Flame Retardant Suit On)
  - #WFH shows the Net has become a utility.
  - It should be regulated as such.
  - 21st Century version of Rural Electrification Project

5/14/2020
48

VIRGINIA TECH.

https://www.forbes.com/sites/steveandriole/2020/03/30/its-time-for-an-internet-for-all-public-utility-before-corona-crashes-it/

Your Work Computer Became Your Home Computer

- Hopefully not!
- WFH not new but # of WFH computers has INCREASED
- Will your company tools work outside of your work network?
  - Active Directory?
  - Authentication? 2 factor?
  - Software Licensing?
  - Virtual Private Network (VPN)?

VIRGINIA TECH.

And Now Some Geek-Speak

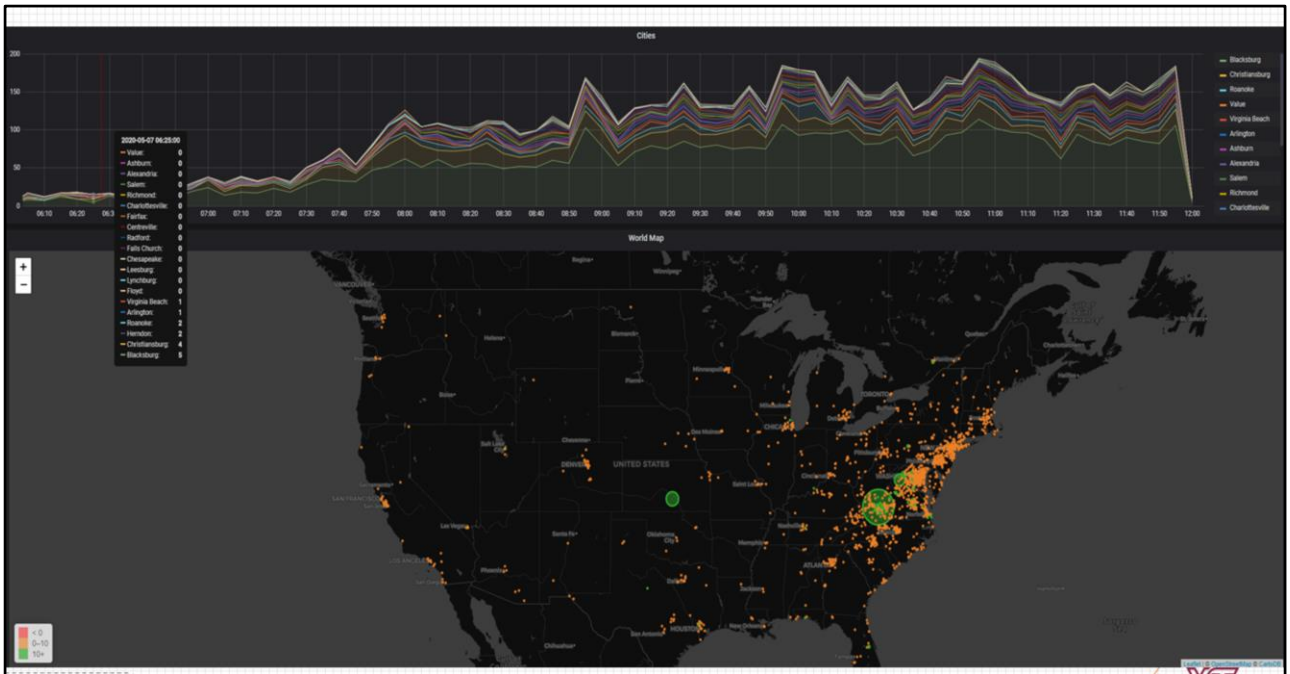
- Can your IT scan computers at your house?
  - Probably not. May be blocked by your ISP
- Can you "disconnect" a host from your network?
  - ISP will get abuse complaints not your org.
- What network traffic visibility exists from computers at your house?
  - None probably unless you require VPN.
- What type of logs will you need to collect in this new WFH environment?

VIRGINIA TECH.

VT IT Security Considerations

- ITSO team – 2 were already teleworking, 5 switched over 3/11-3/20
  - Work meeting, 1-1 meetings, Weekly Zoom Happy Hour
- Monitoring systems – no change
- Endpoint Visibility changed
  - **Expanded VPN to handle extra load. Gives us local IP and userid**
  - Home ISP can interfere with scanning remote hosts, cutting off access, etc.
  - ISP might get abuse complaints and we won't know it
  - Some network log info can't be collected because some of it isn't in our net anymore.

VIRGINIA TECH.



VIRGINIA TECH.

Your Home Computer Became Your Work Computer - 1

- If you use your home computer for work, you must follow your office's security requirements on it.
- **Create a separate userid for work stuff.** Keeps personal separate from work.
  - Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.
- When you're done #WFH, you can delete that account

VIRGINIA TECH.

Your Home Computer Became Your Work Computer - 2

- You become your Help Desk, system support group
- Does your home computer meet any regulatory requirements imposed on the data you use?

VIRGINIA TECH.

POLICIES AND STANDARDS BY SUBJECT

ACCEPTABLE USE

University numbered policies

- 7000 - Acceptable Use and Administration of Computer and Communication Systems
- 4082 - Appropriate Use of Electronic Personnel and Payroll Records
- 4325 - Alternate Work Site and Telework Policy
- 5215 - Sales, Solicitation and Advertising on Campus

Commonwealth of Virginia policies

- Department of Human Resource Management Policy 1.75, Use of the Internet and Electronic Communications Systems

Standards

- Acceptable Use of Information Systems at Virginia Tech

SECURITY AND DATA PROTECTION

University numbered policies

- 7010 - Policy for Securing Technology Resources and Services
- 7025 - Safeguarding Nonpublic Customer Information
- 7030 - Policy on Privacy Statements on Virginia Tech Web Sites
- 7035 - Privacy Policy for Employees' Electronic Communications
- 7105 - Policy for Protecting University Information in Digital Form
- 7200 - University Information Technology Security Program

Standards

- Standard for Securing Web Technology Resources
- Virginia Tech Risk Classifications
- Minimum Security Standards
- Standard for High Risk Digital Data Protection
- Standard for Information Technology Logging

IDENTITY MANAGEMENT

University numbered policies

- 7040 - Policy and Procedures for Personal Credentials for Enterprise Electronic Services

Standards

VIRGINIA TECH.

Virginia Tech IT Policies & Standards - https://it.vt.edu/resources/policies.html
Virginia Tech Policy 7010 Policy for Security Technology Resources and Services - https://policies.vt.edu/7010.pdf
Virginia Tech Risk Classifications - https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf
Virginia Tech Minimum Security Standards for Endpoints, Servers, Applications - https://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf

2.0 Policy

Information technology resources and services must be securely maintained and must be associated with an individual who is responsible for ensuring their continued security.

2.1 Scope

This policy applies to any technology resource or service that:

- Is owned or managed by the university;
- Is connected to the university network;
- Connects to another university technology resource or service; or
- Stores university data or information.

This policy applies whether the network connections are remote or campus-based.

The owner of a technology resource may use it at his or her discretion; however, once that device is connected to the university network or other technology resource or service or is used to store university data, it is subject to applicable laws and regulations and to university policies.

VIRGINIA TECH.

Low Risk

Data and systems are classified as low risk if they are not considered to be moderate or high risk, and:

1. The data is intended for public disclosure, or
2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.

Moderate Risk

Data and systems are classified as moderate risk if they are not considered to be high risk and:

1. The data is not generally available to the public, or
2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.

High Risk

Data and systems are classified as high risk if:

1. Protection of the data is required by law/regulation, and
2. Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed; or
3. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

VIRGINIA TECH.

STANDARDS	WHAT TO DO	L	M	H	CSC
Patching	Apply security patches within 30 days of publish. BigFix is recommended. Use a supported OS version.	✓	✓	✓	3
Whole Disk Encryption	Use FileVault2 for Mac. Use BitLocker for Windows. Consider Veracrypt if applicable. Recommended for low-risk endpoints.		✓	✓	13
Malware Protection	Install antivirus (e.g., Windows Defender) and configure to automatically update and run scheduled scans.	✓	✓	✓	8
Backup	Backup local user data at least weekly. Consider using Network Backup Service.	✓	✓	✓	10
Inventory	Register your endpoint with departmental inventory system.	✓	✓	✓	1

STANDARDS	WHAT TO DO	L	M	H	CSC
Firewall	Enable host-based firewall in default deny mode and permit only the minimum necessary services.	✓	✓	✓	9
Equipment Disposal	All university-owned equipment must go through Surplus Property for disposal.	✓	✓	✓	1
Credentials and Access Control	Configure workstations and laptops to prohibit anonymous access. Enforce password age, length, and complexity. Require password-protected screen savers, with a recommended 15-minute time for inactivity, or lock device before leaving it unattended.	✓	✓	✓	4, 16
Configuration Management	Install BigFix or equivalent (Kaseya)			✓	3, 5
Regulated Data Security Controls	Implement PCI DSS, FISMA, or export controls as applicable.			✓	12 13 14
Centralized Logging	Forward logs to a remote log server. Use of the university's centralized log server is recommended (required for division of IT endpoints). Review logging standard for additional			✓	6

VIRGINIA TECH.

Simple Steps to Protect Your Computer

- Password protect your userid, screen lock
- Update your OS & software
- Think before click
- You have a firewall already
- Adjust browser security, privacy settings

- Encrypt sensitive data
  - Use Microsoft Office tool
  - Remember your password!
- https://www.us-cert.gov/ncas/tips/ST15-002 "How to Secure Your Home Network"
- https://privacy.net/how-to-secure-your-computer/

https://privacy.net/how-to-secure-your-computer/

VIRGINIA TECH.

Top Tips - For Video Conference Attendees

- Update Software
- Audio / Video Settings
- Background
- Don't Share Invites
- Screenshots

5/14/2020

60

VIRGINIA TECH.

https://4help.vt.edu/sp?id=kb_article&sys_id=1c56da51db5c9fc41c1e86171b961980#Best

Top Tips - For Video Conference Organizers

- Updated Software
- Passwords
- Review Attendees
- Lock Conference
- Eliminate Disruptors

- Audio / Video Settings
- Screensharing
- Background
- Inform Recording
- Disable Screenshots

5/14/2020
61

VIRGINIA TECH.

https://zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf – Best Practices for Securing Your Zoom Meeting

A Plan For Videoconferencing (VC)

- Align with your office policies, standards
  - Protect sensitive data at rest and in transit
- Align Endpoint Security
- Align default setting of Video Conference tool to your requirements
  - Classroom/training vs. Business Topics vs. Video Happy Hour

5/14/2020
62

VIRGINIA TECH.

https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF - NSA Selecting and Safely Using Collaboration Services for Telework

Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Cisco Webex®[9]	a, b, c, d, e	Y[1]	Y	Y[12]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™[10]	a, b, c, d	N	Y	Y[1]	Y[1]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®[11]	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Mattermost™[12]	a, b, c, e	Y	Y	Y[2]	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®[13]	a, c, d, e	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®[14]	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™[15]	a, c, d, e	Y[4]	Y[4]	Y	Y	N	Client – Y Server – N[3]	N	None
Slack®[16]	a, c, d, e	N	Y	Y	Y	N[3]	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®[17]	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®[18]	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom®[19]	a, b, c, e	Y[14]	Y	N	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Table of Assessments against Criteria

VIRGINIA TECH.

128.173.200.142 - Mozilla Firefox

NP3F1C76 / 128.173.200.142

hp LaserJet 4200

Information | Settings | Networking

CONFIGURATION
- Network Settings
- Other Settings
- Privacy Settings
- Select Language

SECURITY
- Settings
- Authorization
- Mgmt. Protocols

DIAGNOSTICS
- Network Statistics
- Protocol Info
- Configuration Page

Other Links
- Help
- Support
- HP Home

Settings

Status | Wizard | Restore Defaults

Authorization

Administrator Password:	Not Set
Jetdirect Certificate:	Installed
Access Control:	Disabled

Web Interface

Encrypt All Web Communication:	Disabled
Encryption Strength:	Low (DES-56-bit, RC4-128-bit or 3DES-168-bit)

SNMPv1/v2

Status:	Enabled
Get Community Name:	Not Set (Defaults to "public")
Set Community Name:	Not Set (Defaults to "public")

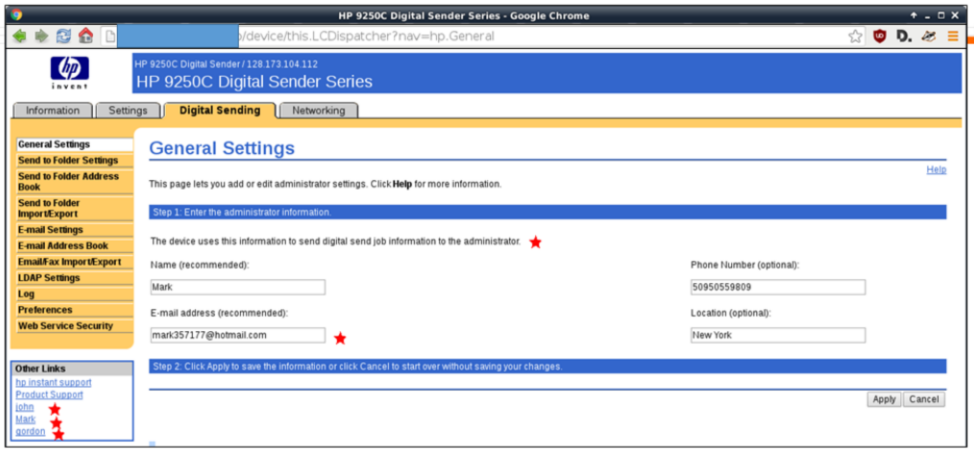
SNMPv3

Status:	Disabled

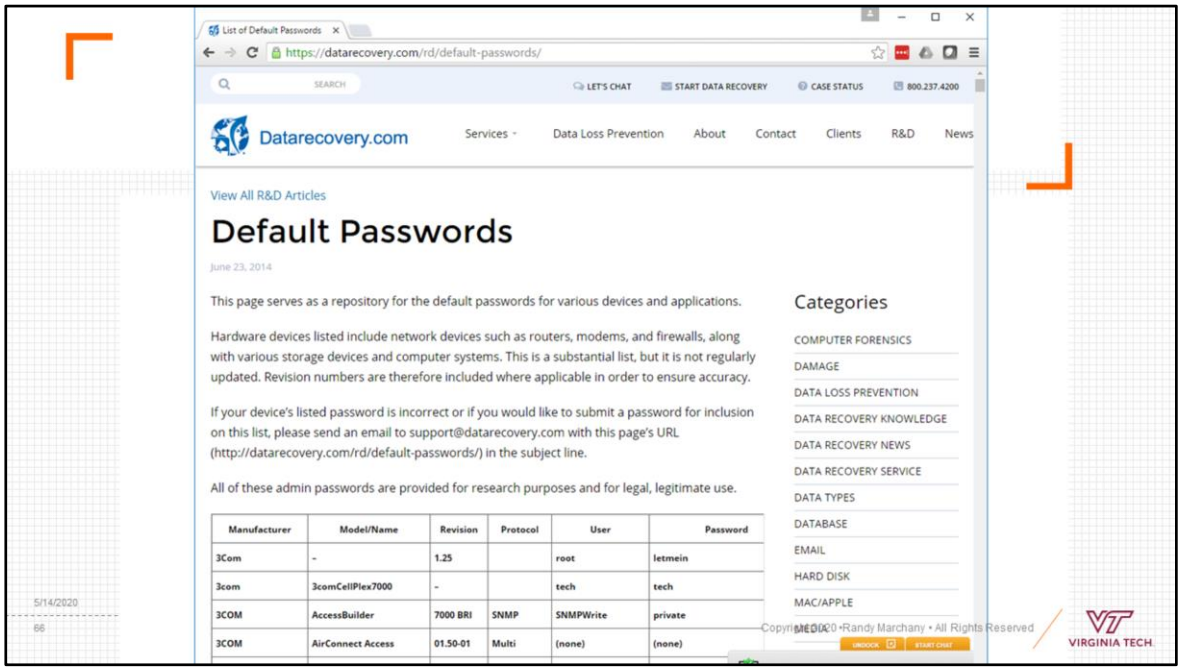
Other Protocols

IPX/SPX:	Enabled
AppleTalk:	Enabled
DLC/LLC:	Enabled
9100 Printing:	Enabled
LPD Printing:	Enabled
IPP Printing:	Enabled
FTP Printing:	Enabled
SLP Config:	Enabled
mDNS:	Enabled
Multicast IPv4:	Enabled
RCFG:	Enabled

VIRGINIA TECH.



VIRGINIA TECH.



List of Default Passwords

https://datarecovery.com/rd/default-passwords/

SEARCH | LET'S CHAT | START DATA RECOVERY | CASE STATUS | 800.237.4200

Datarecovery.com

Services | Data Loss Prevention | About | Contact | Clients | R&D | News

View All R&D Articles

Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

If your device's listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page's URL (http://datarecovery.com/rd/default-passwords/) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

Manufacturer	Model/Name	Revision	Protocol	User	Password
3Com	-	1.25		root	letmein
3com	3comCellPlex7000	-		tech	tech
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite	private
3COM	AirConnect Access	01.50-01	Multi	(none)	(none)

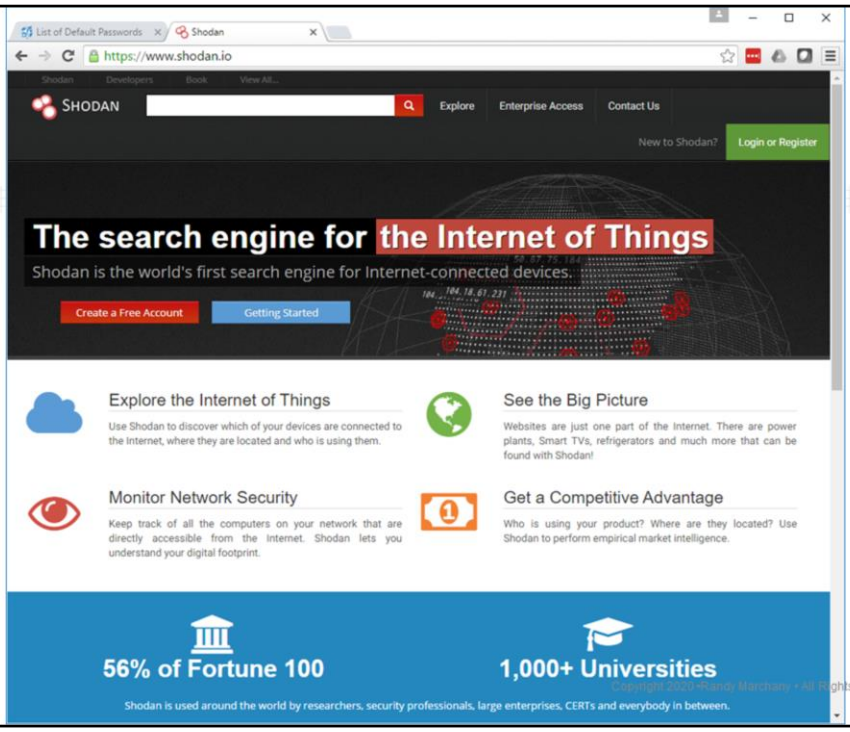
Categories

COMPUTER FORENSICS
DAMAGE
DATA LOSS PREVENTION
DATA RECOVERY KNOWLEDGE
DATA RECOVERY NEWS
DATA RECOVERY SERVICE
DATA TYPES
DATABASE
EMAIL
HARD DISK
MAC/APPLE
MEDIA

UNDOCK | START CHAT

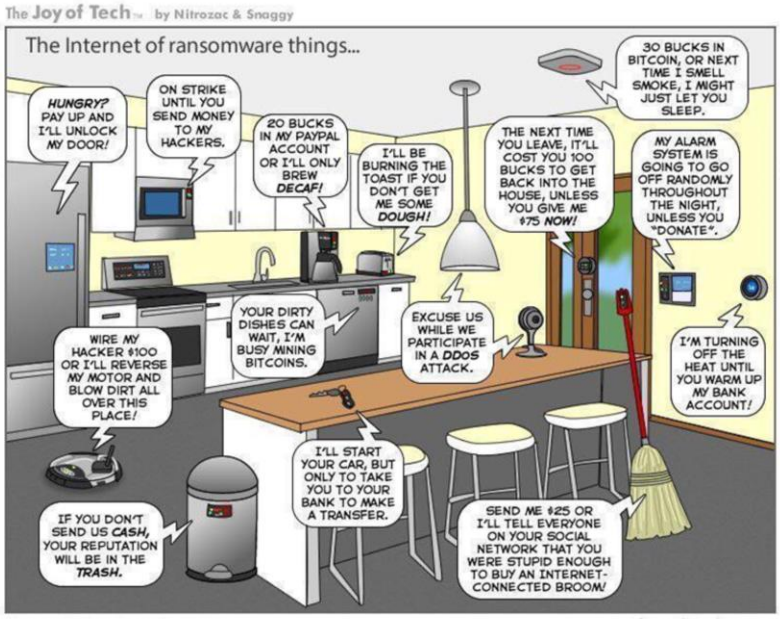
VIRGINIA TECH

https://datarecovery.com/rd/default-passwords/



VIRGINIA TECH

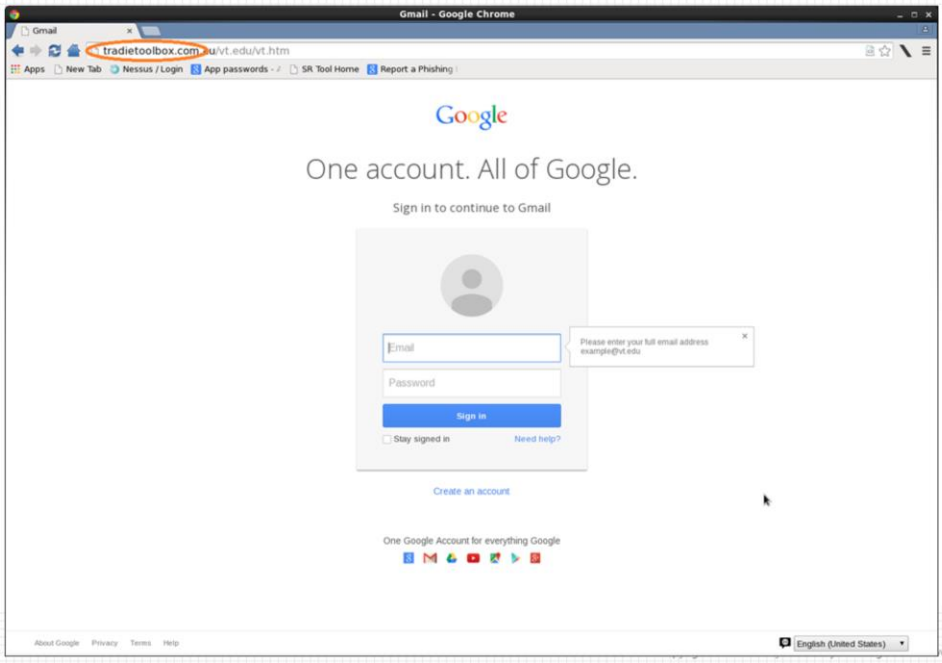
The Joy of Tech by Nitrozac & Snaggy



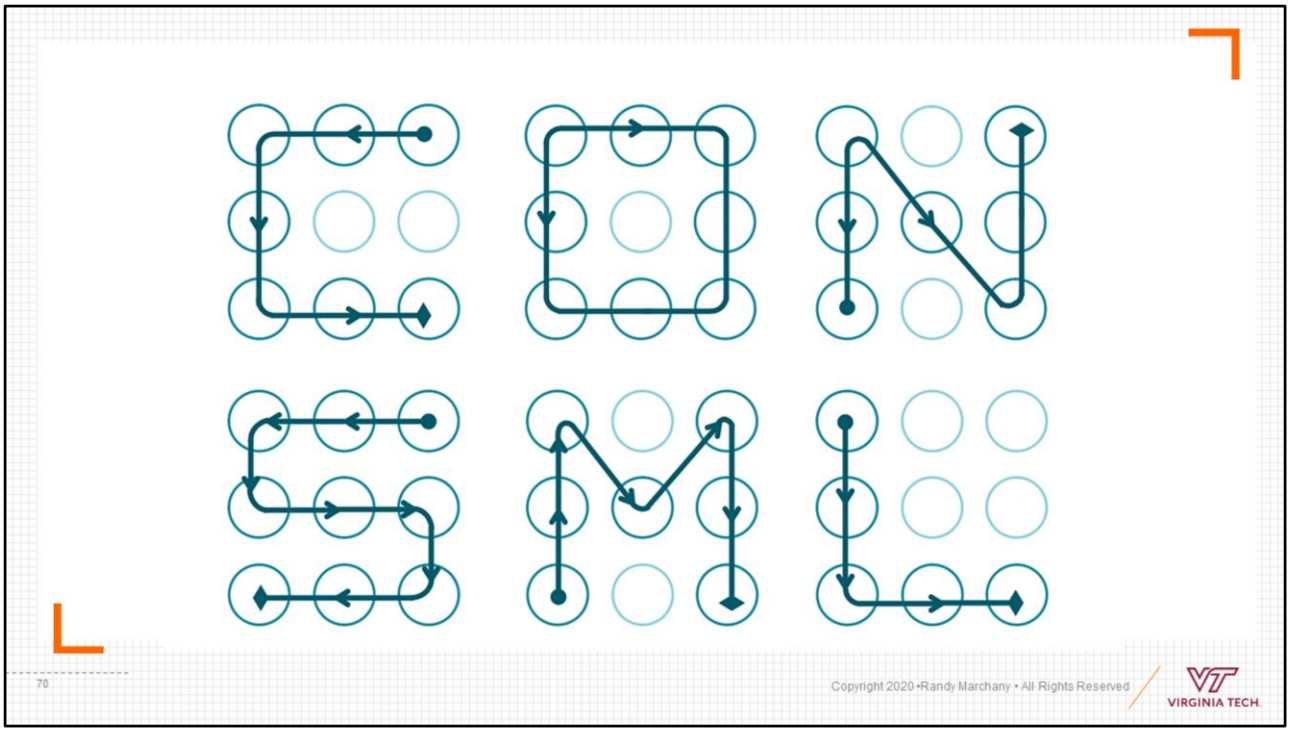
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech

joyoftech.com

VIRGINIA TECH



VIRGINIA TECH.



Source: Brad Tilley, VA Tech IT Security Office

Phonology

- How we form sounds and group consonant and vowel patterns.
- CVCCVC is "The Batman Pattern". There are many other popular patterns.
  - BATMAN
  - (CATWOM)AN
- Sometimes broken into grams (JtR does this) rather than CVC patterns.
  - Bigrams (th, he)
  - Trigrams (the, ing)
  - Quadrigrams (that, ther)

71

Source: Brad Tilley, VA Tech IT Security Office

Do use different passwords for different site

- NIST says "Longer is better"
- Example: ***thisisareallylongpassword-gmail, thisisreallylongpassword-amazon***

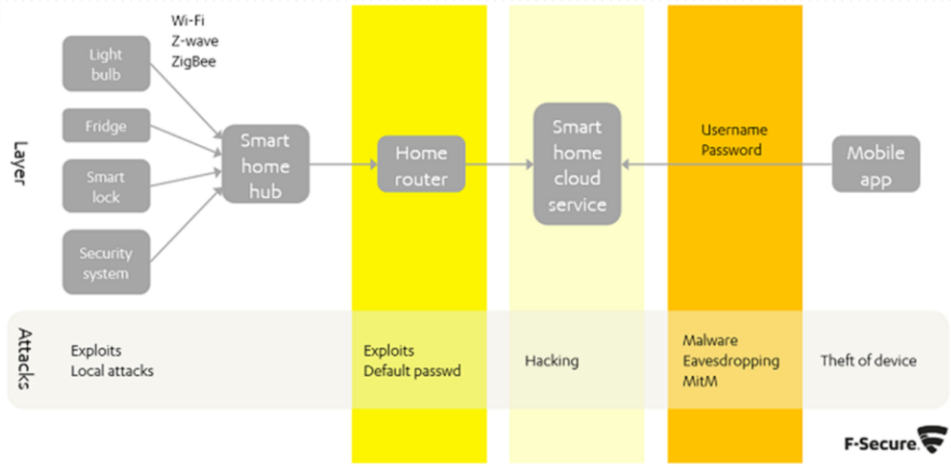
- Your email account is the key to the kingdom.
  - Compromise that, everything falls.
  - Request resets from bank, Facebook, Twitter, etc.

72

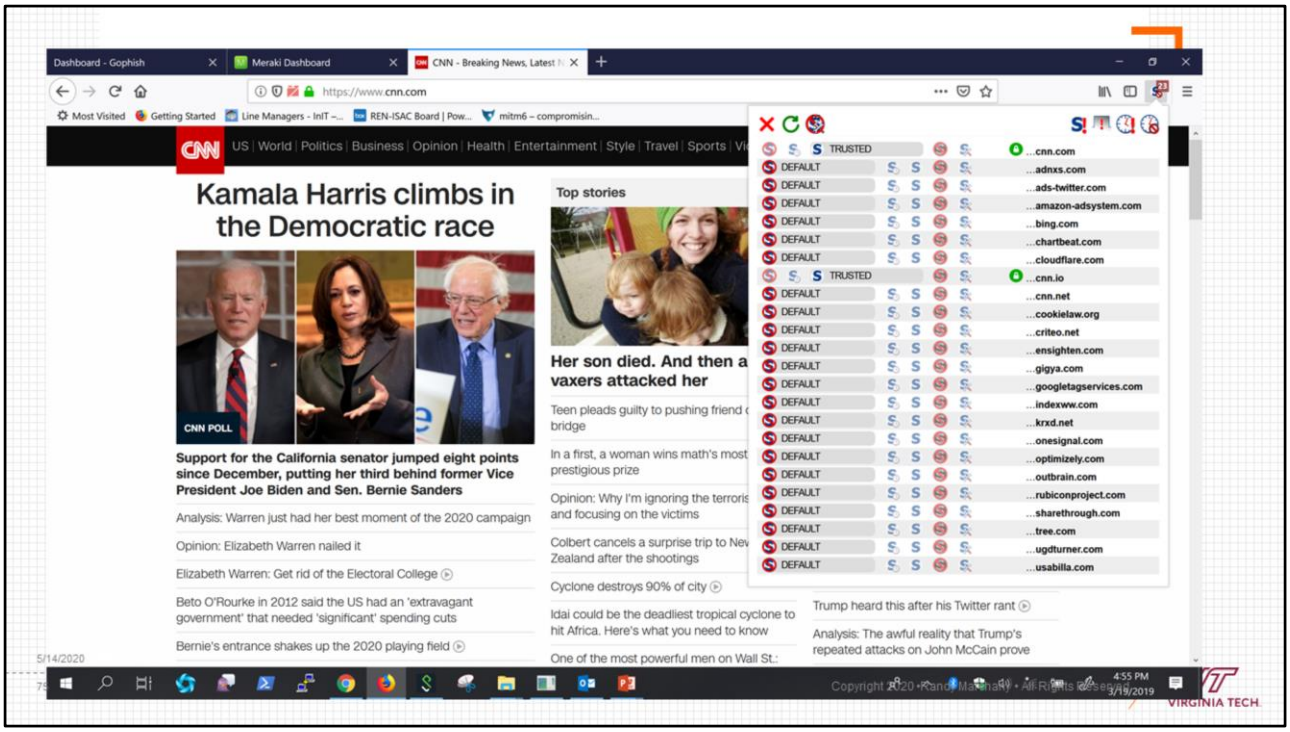
Source: Brad Tilley, VA Tech IT Security Office

VIRGINIA TECH

Protect your home network



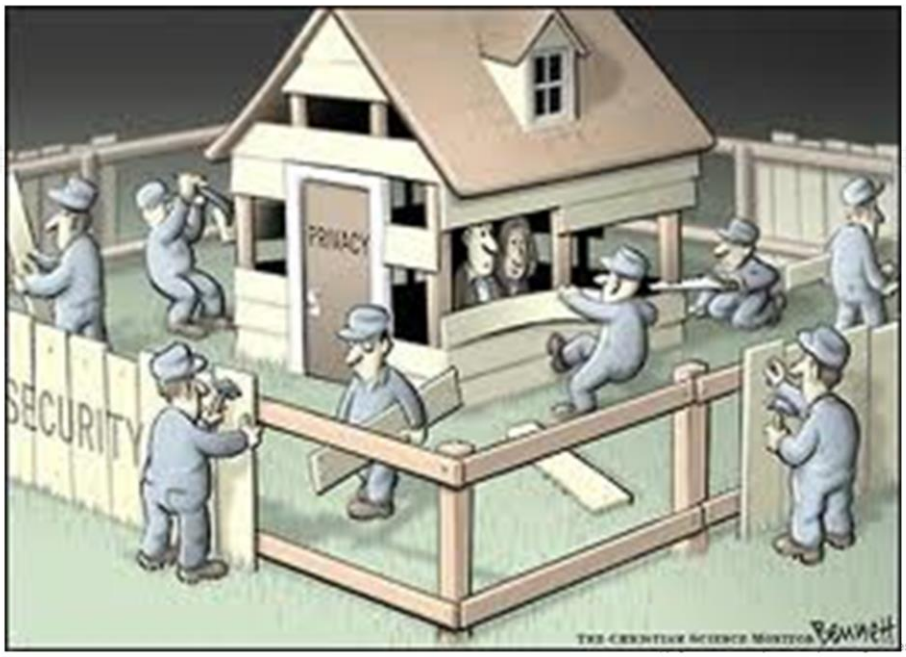
VIRGINIA TECH


Dashboard - Gophish
Meraki Dashboard
CNN - Breaking News, Latest N
https://www.cnn.com
Most Visited
Getting Started
Line Managers - InIT –...
REN-ISAC Board | Pow...
mitm6 – compromisin...
CNN
US | World | Politics | Business | Opinion | Health | Entertainment | Style | Travel | Sports
Kamala Harris climbs in the Democratic race
CNN POLL
Support for the California senator jumped eight points since December, putting her third behind former Vice President Joe Biden and Sen. Bernie Sanders
Analysis: Warren just had her best moment of the 2020 campaign
Opinion: Elizabeth Warren nailed it
Elizabeth Warren: Get rid of the Electoral College
Beto O'Rourke in 2012 said the US had an 'extravagant government' that needed 'significant' spending cuts
Bernie's entrance shakes up the 2020 playing field
Top stories
Her son died. And then a
vaxers attacked her
Teen pleads guilty to pushing friend
bridge
In a first, a woman wins math's most
prestigious prize
Opinion: Why I'm ignoring the terroris
and focusing on the victims
Colbert cancels a surprise trip to Ne
Zealand after the shootings
Cyclone destroys 90% of city
Idai could be the deadliest tropical cyclone to hit Africa. Here's what you need to know
One of the most powerful men on Wall St.:
Trump heard this after his Twitter rant
Analysis: The awful reality that Trump's repeated attacks on John McCain prove
TRUSTED ...cnn.com
DEFAULT ...adnxs.com
DEFAULT ...ads-twitter.com
DEFAULT ...amazon-adsystem.com
DEFAULT ...bing.com
DEFAULT ...chartbeat.com
DEFAULT ...cloudflare.com
TRUSTED ...cnn.io
DEFAULT ...cnn.net
DEFAULT ...cookielaw.org
DEFAULT ...criteo.net
DEFAULT ...ensighten.com
DEFAULT ...gigya.com
DEFAULT ...googletagservices.com
DEFAULT ...indexww.com
DEFAULT ...krxd.net
DEFAULT ...onesignal.com
DEFAULT ...optimizely.com
DEFAULT ...outbrain.com
DEFAULT ...rubiconproject.com
DEFAULT ...sharethrough.com
DEFAULT ...tree.com
DEFAULT ...ugdturner.com
DEFAULT ...usabilla.com
5/14/2020
4:55 PM
3/19/2019
Copyright 2020 - Randy McNally - All Rights Reserved
VIRGINIA TECH.

Most Common Security Mistakes Made by Individuals (2001)

- Poor password management
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- Not installing anti-virus software
- Laptops on the loose
- Blabber mounts
- Plug and Play without protection
- Not reporting security violations
- Always behind the times (OS, application patches)
- Keeping an eye out inside the organization

VIRGINIA TECH



https://en.wikipedia.org/wiki/Clay_Bennett_(cartoonist)

Contact Information

- Randy Marchany
- VA Tech IT Security Office & Lab
- 1300 Torgersen Hall
- VA Tech
- Blacksburg, VA 24060
- 540-231-9523
- marchany@vt.edu
- http://security.vt.edu
- Twitter: @randymarchany
- Blog: randymarchany.blogspot.com

- To see the speaker notes (annotations) in this PDF, open this file, click on "Comment" button in the upper right. Click on "Annotations" to see the hyperlink references in the slides.

VIRGINIA TECH

Security without Barriers: Enabling Secure Remote Access for Your Campus

Q&A

Kurt Eisele-Dyrli
Web Seminar Editor
University Business

Randy Marchany
University IT Security Officer
Virginia Tech

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

Have a question for our presenters? Submit it through the Q&A at the right.

Q&A

UB University Business

FIREEYE

University Business is the leader in editorial coverage of news, trends and current issues in higher education.

Subscribe for FREE and stay up-to-date through our print magazine, digital edition, enewsletters and web seminars.

Print magazine

Digital edition and website

Web seminars

UB Daily, and other enewsletters

UB University Business

FIREEYE

Thank you for joining us!

The archive recording of this web seminar will be available for you to review, or share with members of your team, at:

http://www.UniversityBusiness.com/Web-Seminars

You will also receive an email with a link to the slides.

UB University Business

FIREEYE