



Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Sept. 11, 2019



ISOAG Sept. 11, 2019 Agenda

I. Welcome and Opening Remarks

Mike Watson, VITA

**II. Updates to Dynamic Approval
Workflow for KSE**

Jeff Limones, SAIC

III. SAIC Incident Response

Tanya Nacey, SAIC

IV. Capture the Flag

David Raymond, VA Cyber Range

V. Virginia and Google Cloud

Scott Fleming, Google

VI. Security Challenge Game

Marlon Cole, VITA

VII. Upcoming Events

Mike Watson, VITA



Dynamic Workflow - ISO Approvals

Team: MSI Innovation and Solutions
Team

Jeff Limones, SAIC

Sept. 11, 2019

VITA ISOAG



Virginia Information Technologies Agency

MSI Cybersecurity Response Team

Tanya Nacey, SAIC

Security Incident Management

Sept. 11, 2019

VITA ISOAG



Security incident management

The SAIC MSI Cybersecurity Response Team [CSIRT]

- Provides 24x7 computer security incident response services to the Commonwealth of Virginia, state agencies, and VITA locality customers as needed
- Our main focus is on efficient management of the security incident lifecycle when security events occur and during potential cybersecurity-related emergencies
- Particularly as they cross over into the seven other service tower supplier [STS] service areas and to avoid recurrence



Security incident management

The SAIC MSI Cybersecurity Response Team [CSIRT]

- Our strengths lie in collaborative management with our STS partners to mitigate the potentially serious effects of a severe computer security-related problem
- To achieve this goal, we concentrate our efforts and respond to computer security incidents to regain control, minimize damage, and providing effective incident response and recovery
- The lifecycle concludes with MSI CSIRT recommendations for corrective action where controls may have failed, thus preventing future computer security incidents from recurring



Security incident management

- All security incidents are handled as SEV 1 priority and addressed at a regular call cadence with the CSIRT during the security incident 24/7/365
- CSIRT POC's are service tower ISO's who designate appropriate technical engineers to respond to a security event at any point in time
- Each security incident is investigated by ATOS and often crosses over to another tower through the MSI
- MSI cybersecurity response and JOC teams support the efficient handling and management of the security incident lifecycle to maintain fluidity for prompt containment, remediation, recovery and assessing root cause
- VITA's Archer system holds all security incidents for the commonwealth



Security incident management

- The Keystone Edge system holds all security incident tasks assigned to a service tower for action required during the commission of a security incident:
 - Investigation
 - Containment
 - Remediation
 - Recovery
 - Root cause analysis
- The Keystone Edge system holds all corresponding security incident service level agreements [SLAs], both related and shared between service towers



Security incident service levels

Service level		Exp	Min
Security incident containment	Percentage of the time the supplier takes to contain security incidents within the applicable timeframes (≤ 4 hours)	99.90%	99.70%
Security incident resolution	Percentage of time the supplier takes to resolve security incidents within the applicable timeframes (≤ 72 hours)	98.50%	98.50%



CSIRT upcoming event

EXERCISE! EXERCISE! EXERCISE! EXERCISE!

- A tabletop exercise will be held the last week of October, and hosted by the MSI CSIRT
- Agencies will receive participation credit in the form of a VITA certification to produce for audit compliance
- STS's will also receive participation credit in the form of certification to produce for audit compliance



Questions?

Hands-on hacking: capture-the-flag

David Raymond, Ph.D.
Director, Virginia Cyber Range
draymond@virginiacyberrange.org



VIRGINIA CYBER RANGE

Agenda



- Virginia cyber range overview
- Overview of capture-the-flag (CTF)
- General CTF challenge-solving tips
- CTF challenges by category
- Where to find CTFs to play

Image: <https://masspeaceaction.org/autumn-convergence-agenda-and-workshops/>



VIRGINIA
CYBER RANGE

Virginia Cyber Range: Background

- ❑ Recommended by the Virginia Cyber Security Commission in August 2015
- ❑ Funded by Commonwealth of Virginia on July 1, 2016
- ❑ Now included in annual base budget

2016 Executive Budget Document, Item 224, Paragraph J:

“Out of this appropriation, [two years of funding will be] designated to support a cyber range platform to be used for cyber security training by students in Virginia's public high schools, community colleges, and four-year institutions. Virginia Tech shall form a consortium among participating institutions, and shall serve as the coordinating entity for use of the platform. The consortium should initially include all Virginia public institutions with a certification of academic excellence from the federal government.”





Courseware repository

- ❑ Courses, modules, and exercises for use in HS, CC, and university cybersecurity curricula
 - Instructors/professors can select course content in full or *a la carte*
- ❑ Grants offered for courseware development



Exercise area

- ❑ Menu of per-student exercise environments for use in cybersecurity courses
- ❑ Working towards team-based offensive and defensive, scenario-based environments
- ❑ Capture-the-flag infrastructure for cybersecurity competitions



Community of purpose

- ❑ Consortium governance
- ❑ Convene workshops and conferences to “teach the teachers” and share best practices
- ❑ Helping to expand NSA/DHS CAE certification among Virginia colleges and universities

Leveraging the public cloud

Design requirements:

- Difficult to predict resource requirements
- Completely automatable
- Cost effective
- Short-term surge capacity
- Available anywhere
- Web portal for access to content
 - Role-based access
 - Login to see user-specific content
 - Students just need a web browser and internet connection!



Why the Cloud?

- *Unlimited scalability!*
- Quick start-up phase
- Low capital investment
- Rapid scalability
- Surge capacity
- Location independent
- Highly automated
- Pay as you use



VIRGINIA
CYBER RANGE

Virginia cyber range way ahead

- Continuing to evolve functionality
- Expanding capture-the-flag (CTF) infrastructure
- Expanding content library
 - More high school and college-level courseware
 - More flexible exercise environments

*Expanding beyond Virginia . . .
... and beyond academia.*



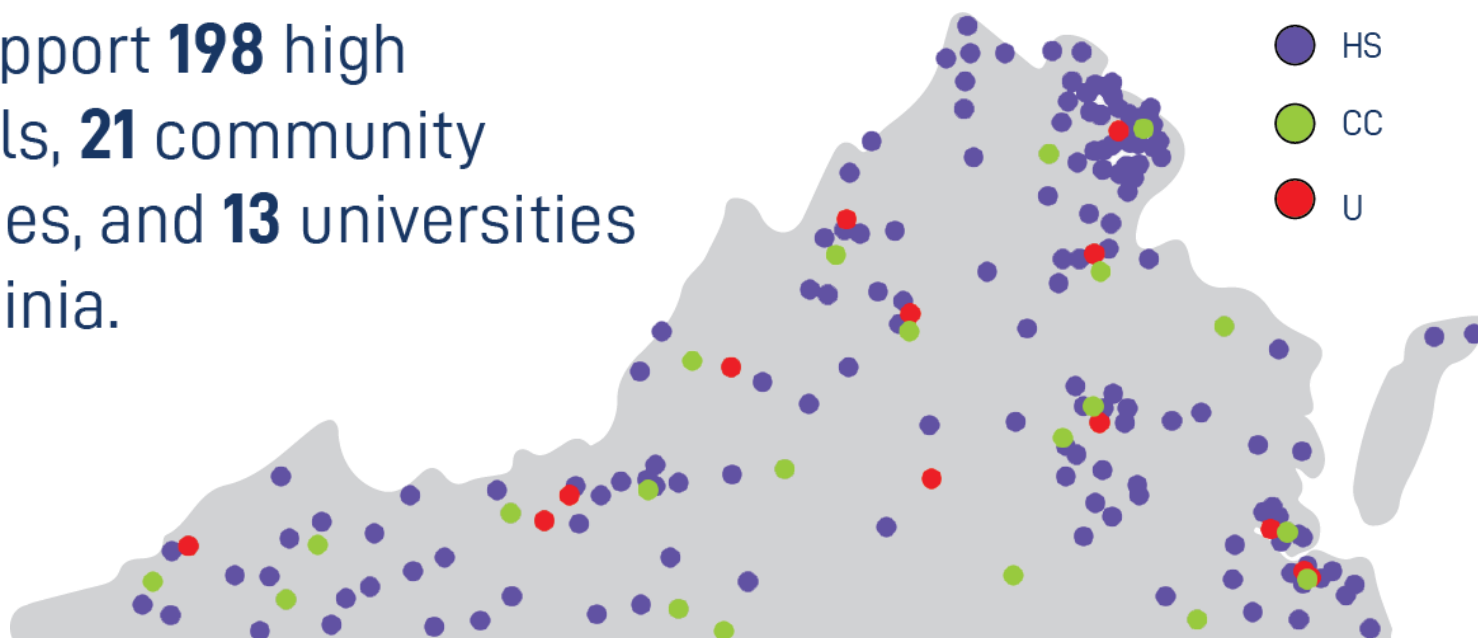
U.S. CYBER RANGE



VIRGINIA
CYBER RANGE

Schools supported

We support **198** high schools, **21** community colleges, and **13** universities in Virginia.



* Each dot represents a different Virginia high school, community college, or university.

What is *Capture-the-flag*?

- ❑ Cybersecurity competition
 - Can be individual or team-based
 - Sometimes in-person, often remote
- ❑ Various formats
 - *Jeopardy-style, most popular and easiest to create*
 - Attack/defend (red/blue)
 - Example: DEFCON CTF
- ❑ Hosted by:
 - College CTF teams
 - Companies looking for talent
 - DoD and other government agencies
 - *You!*



Why CTFs?

- Good way to spark interest in cybersecurity topics
 - Very popular among high school and college clubs
- A well-designed CTF . . .
 - Caters to wide range of ability levels
 - Encourages independent learning
 - Exercises real-world skills
- Can be used for . . .
 - Teambuilding events
 - Skills assessment
 - Teaching basic skills and problem-solving



Example Jeopardy board (NYU-Poly, 2012)

 Trivia	100	100	100	100	100	
 Recon	100	100	100	400	400	
 Web	100	200	300	400	500	600
 Reversing	100	200	300	400	500	
 Exploitation	200	300	400	500		
 Forensics	200	200	500			
 Networking	100	200	300	400		



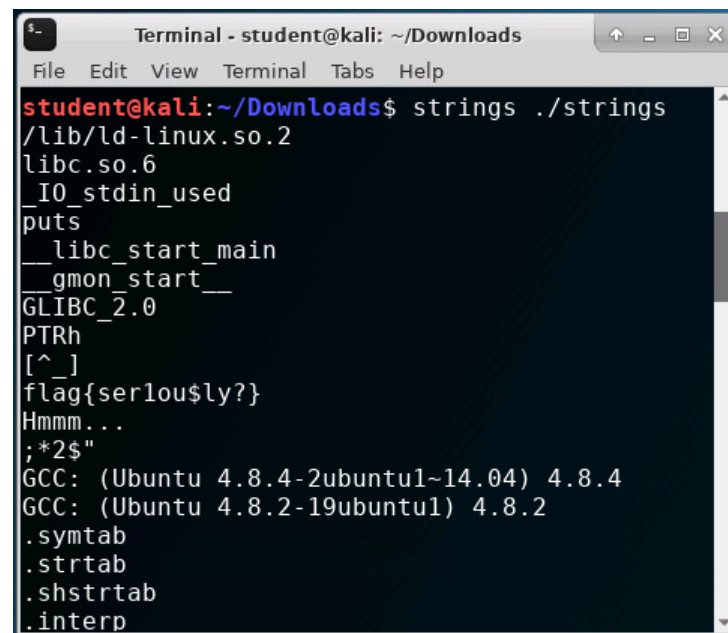
Common challenge types: overview

- **Cryptography**
 - Related to simple ciphers or modern cryptography algorithms
- **Reverse engineering** or binary exploitation
 - Analyzing an executable program to produce a flag
- **Web**
 - Find flag hidden in web traffic or exploit vulnerable web application
- **Digital forensics**
 - Find digital artifacts in a drive image
- **Networking**
 - Find a flag by analyzing captured network traffic
- **Reconnaissance**
 - Answer a question or follow a trail of hints to find a flag



Approaching challenges: general tips

- Look at point values
 - Indicates difficulty level
- Challenge name is almost always a hint
 - Google category along with challenge name
- Read the challenge description carefully
 - Google category along with keywords
- Is there a file? Filename might be a hint
 - File extension or not, run 'file' against it
 - Run 'strings' against it
 - 'cat' the file
 - Open in hex editor
- Any names mentioned?
 - Is the name meaningful?



```
Terminal - student@kali: ~/Downloads
File Edit View Terminal Tabs Help
student@kali:~/Downloads$ strings ./strings
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
puts
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^_]
flag{serlou$ly?}
Hmmm...
;*2$"
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.symtab
.strtab
.shstrtab
.interp
```



Challenge types: cryptography

- Often provided with an encoded message and some hint as to the encoding
- Possible encodings
 - ASCII (decimal or hex values)
 - BASE64/BASE32
 - UUEncoded
 - What else?
- Simple monoalphabetic ciphers
 - Caesar/ROT cipher
 - Substitution cipher
 - These can be easily solved w/out key
 - Frequency analysis!

ABCDEFGHIJKLMNOPQRSTUVWXYZ
MNOPQRSTUVWXYZABCDEFGHIJKL

HI WORLD → TU IADXP

ASCII to Hex ...and other free text conversion tools

Text (ASCII / ANSI)

I gave a cry of astonishment. I saw and thought nothing of the other four Martian monsters; my attention was riveted upon the nearer incident. Simultaneously two other shells burst in the air near the body as the hood twisted round in time to receive, but not in time to dodge, the fourth shell.



VIRGINIA
CYBER RANGE



VIRGINIA
CYBER RANGE

Challenge types: cryptography

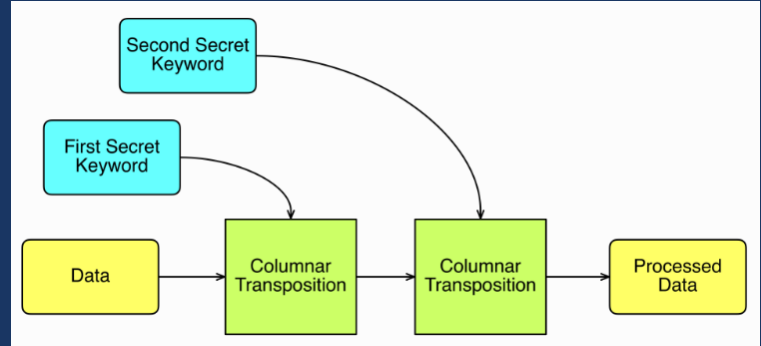
- Polyalphabetic ciphers
 - Vignere cipher
 - Playfair cipher
 - Beaufort cipher
 - Autokey cipher
- Transposition ciphers
 - Railfence cipher
 - Columnar transposition
 - Route cipher
- For more, see:
 - <http://www.crypto-it.net>
 - Khan Academy – Intro to Cryptography

```
T . . . N . . . D . . . G . . .  
. H . U . I . E . K . N . D . M  
. . E . . . T . . . I . . . O .
```

Railfence Cipher

```
6 7 2 3 1 5 4  
A M I D S U M  
M E R N I G H  
T S D R E A M
```

Columnar Transposition



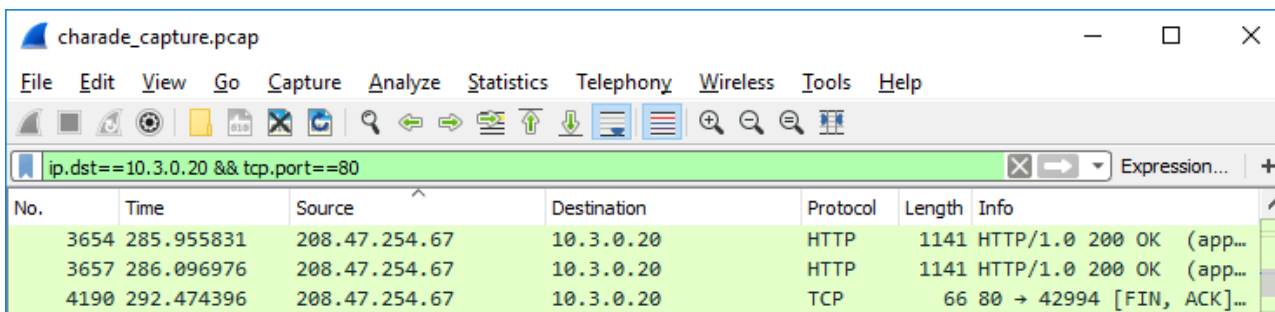
Double Columnar Transposition

Challenge types: networking

- Analyze packet capture to find flag
 - Answer questions related to network traffic
 - “Carve” images and files from packet streams
- Tools
 - Wireshark!
 - Graphical tool for analyzing network traffic
 - Available for Windows, Mac, Linux
 - Download from <https://www.wireshark.org/>
 - tcpdump/windump
 - Command-line tool for examining network traffic
 - ngrep
 - Search for string sin network packets



Wireshark display filters



- Enter filters in textbox
 - Use **Expression** button to get help creating filters
 - Filter box is green for valid filter, red otherwise
- Click **Apply** to apply filter
- Click **Clear** to clear filter



More Wireshark . . .

- **Boolean expressions in filters:**
 - The symbol for logical **AND** in TCP filters is **&&** (you can use **and** and **&&** interchangeably)
 - The symbol for logical **OR** is **||** (you can use **or** and **||** interchangeably)
 - Use parenthesis to form more specific boolean expressions
 - Wireshark generally doesn't care about case except with matching a specific string value.
- Some examples:

Packets from 192.168.1.1	<code>ip.src==192.168.1.1</code>
Packets to and from port 80	<code>tcp.port==80</code>
From 10.10.3.2 to 10.10.3.40	<code>ip.src==10.10.3.2 && ip.dst==10.10.3.40</code>
To/from 10.10.3.2 on port 443	<code>ip.addr==10.10.3.2 && tcp.port==443</code>

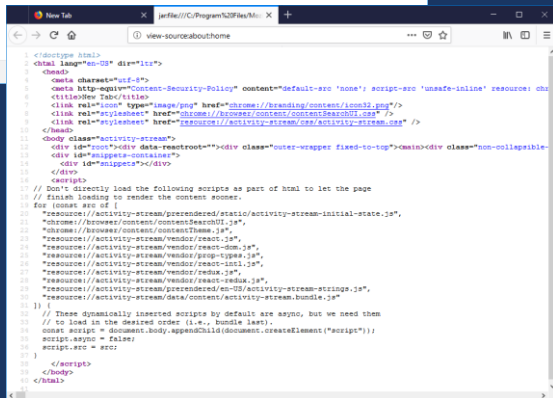
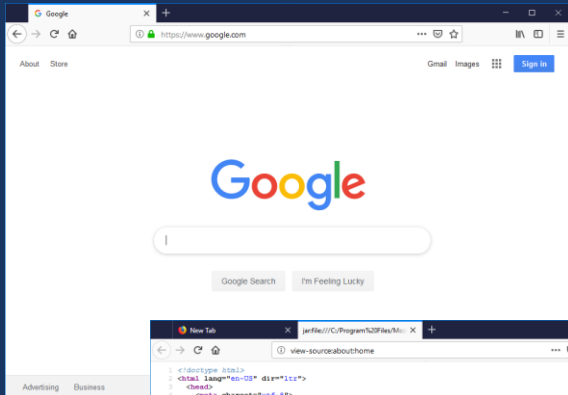


Common protocols

- HTTP
 - In-the-clear web communications
- FTP/TFTP
 - File transfer without encryption
- Telnet
 - Remote login without encryption
- SMTP (port 25)/POP (port 110)/IMAP (port 143)
 - Email communication protocols
- Protocols to ignore (*unless there is a method provided to break encryption*)
 - HTTPS – encrypted web traffic
 - SSH – encrypted remote login
 - SFTP – secure (encrypted) file transfer
 - SMTP (port 465)/IMAPS (port 993)/POP (port 995) – secure email access



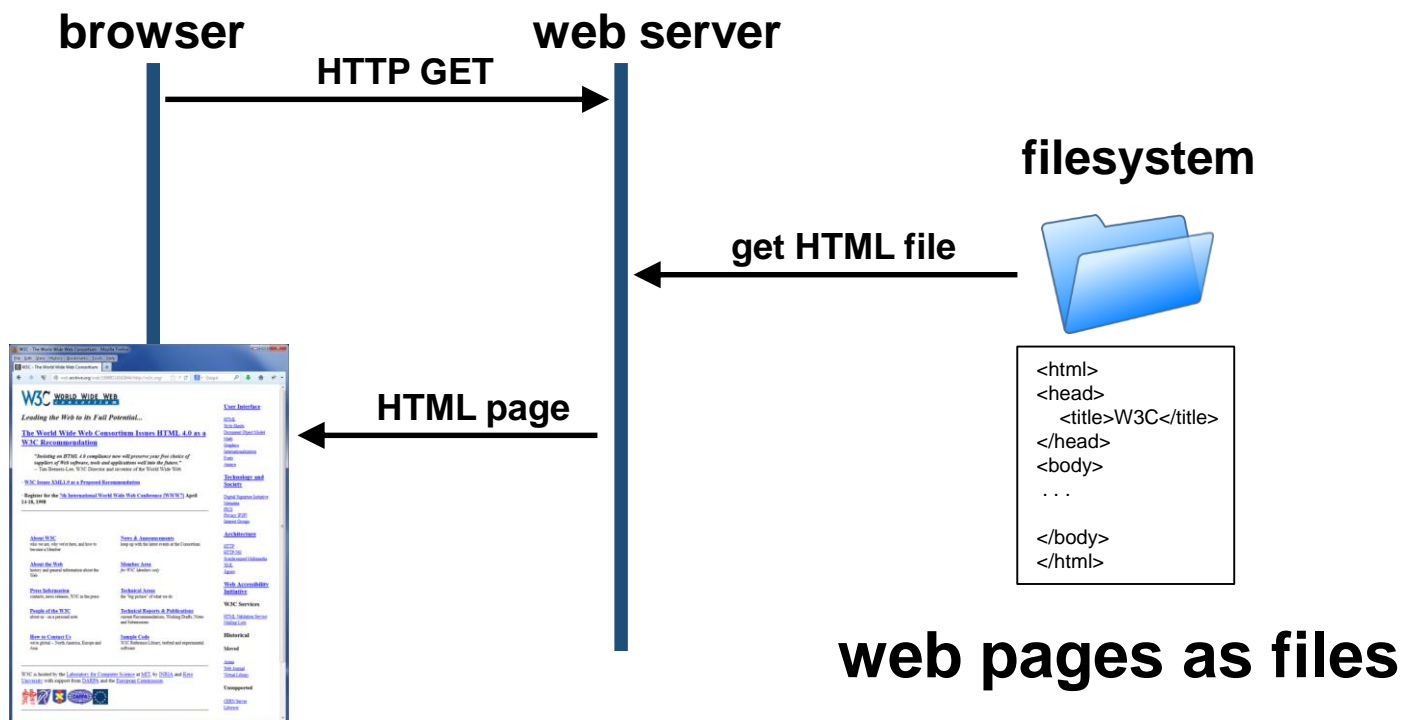
Challenge types: web



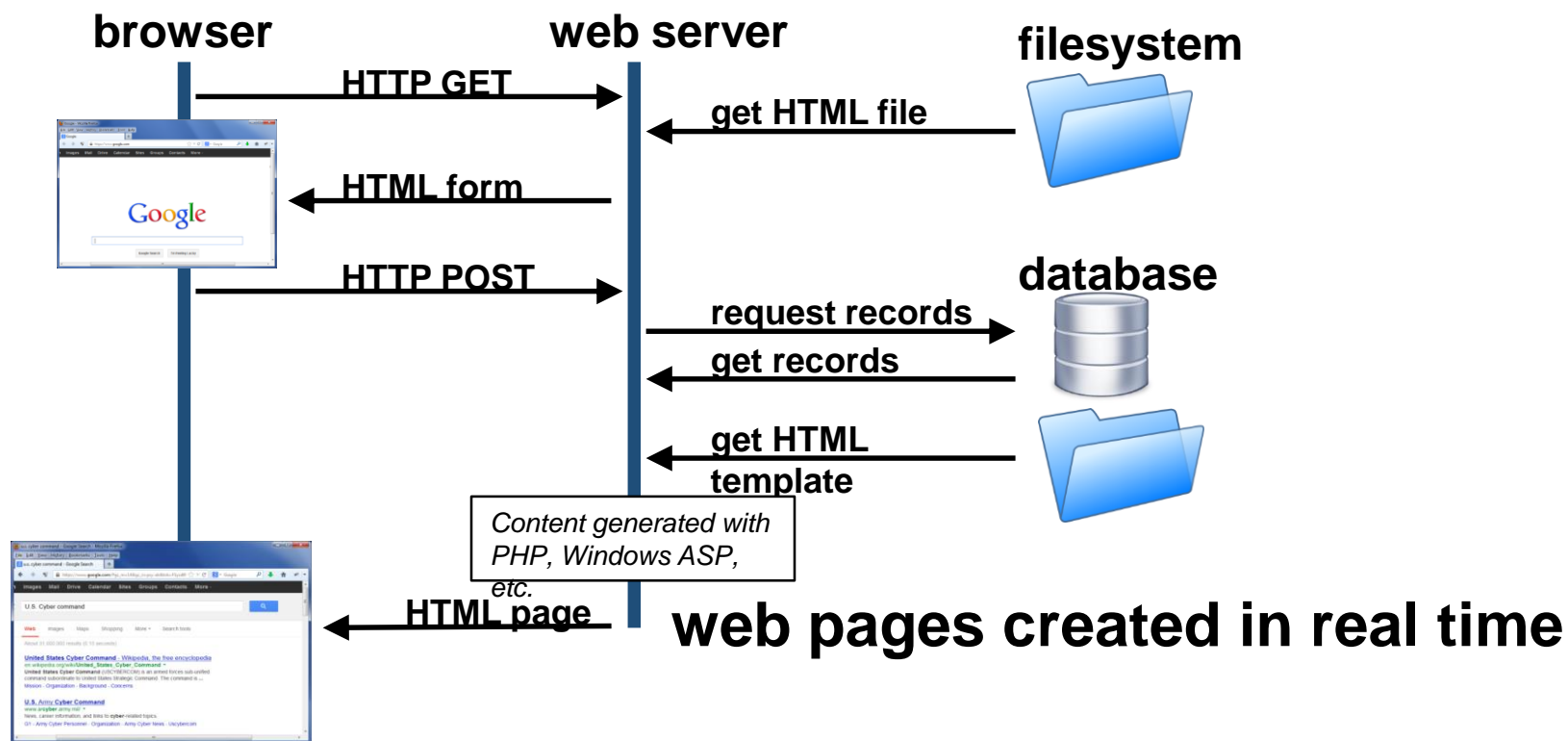
- Easy challenges rely on basic understanding of HTML and how websites work
- Approaches to solving
 - View page source
 - Open 'developer panel'
 - Examine network traffic
 - 'curl' the page examine full response
 - Look for robots.txt
 - Directory traversal attack?
 - *What else?*



Early WWW model



Modern WWW model



Observe web server interaction with Wireshark

- Start Wireshark as root user
- Set display filter: tcp.port==80
- Use browser (or 'curl') to browse to web page
www.sekritskwerl.com
- Stop capture
- Go to top of capture
- Right-click → Follow → TCP stream



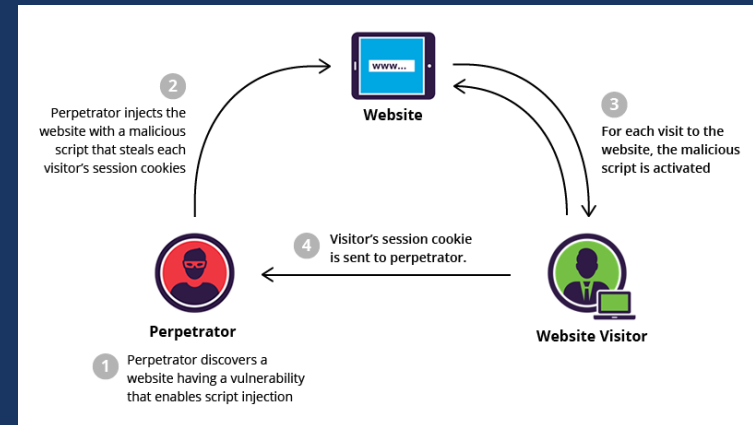
```
Wireshark - Follow TCP Stream (tcp.stream eq 7)...  
GET / HTTP/1.1  
Host: www.acm.org  
Connection: keep-alive  
Cache-Control: max-age=0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36  
Accept-Encoding: gzip, deflate, sdch  
Accept-Language: en-US,en;q=0.8  
Cookie: __ga=GA1.2.1025363245.1463839114; __gat=1; __atuvc=1%7C20; __atuvs=5740698a8661ab2c000; I18N_LANGUAGE="en"  
  
HTTP/1.1 200 OK  
Date: Sat, 21 May 2016 14:08:21 GMT  
Server: Apache-Coyote/1.1  
Content-Type: text/html; charset=UTF-8  
Content-Length: 81816  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
  
<!DOCTYPE html>  
<html lang="en" class="no-js">  
  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible"
```

1 client pkt(s), 61 server pkt(s), 1 turn.
Entire conversation (82 kB) Show data as ASCII Stream 7
Find: Find Next
Hide this stream Print Save as... Close Help

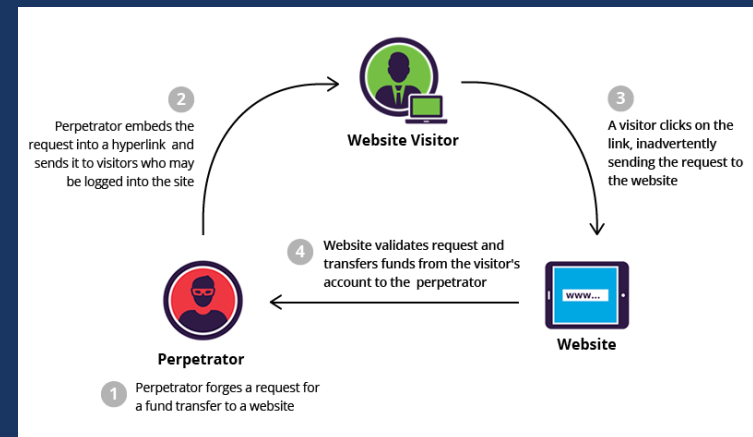


Challenge types: web

- Advanced challenges require advanced techniques to exploit vulnerable web applications
 - Injection attacks (SQL, command)
 - Cross Site Scripting (XSS)
 - Poor coding or site maintenance practices
- What to look for?
 - Buggy php apps
 - Sensitive data exposure
 - Version control artifacts
 - Broken authentication
 - Default installations
 - Inclusion vulnerabilities



Cross Site Scripting



Cross Site Request Forgery



Challenge types: web

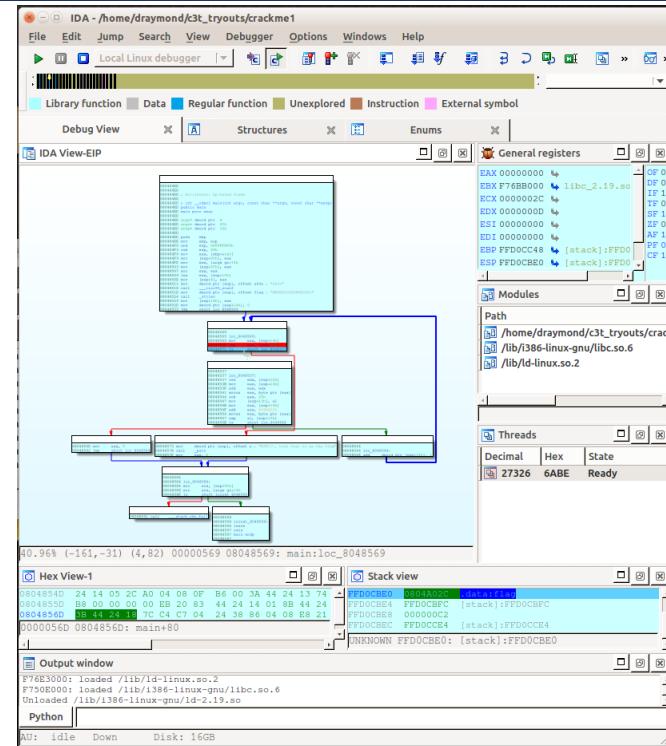
Tools:

- Web browser w/ developer tools to examine site and scripts
- Wireshark/tcpdump to examine packets
- ngrep to search for strings in packet captures
- Web proxy to intercept and change web interactions
 - OWASP ZAP Proxy
 - BurpSuite



Challenge types: reverse engineering

- Analyze or modify an executable program to reveal the flag
 - You are only provided the binary application; no source code
 - It helps to know (and a good way to learn):
 - assembly language
 - computer organization/architecture
- Common tools
 - objdump – Linux command-line disassembler
 - gdb – Linux command-line debugger
 - IDA Pro – commercial disassembler and decompiler (expensive, but demo versions free)
 - Ghidra – new open-source tool created by the National Security Agency



Reverse engineering – entry level challenges

- Use 'strings' to see if the flag is obvious
`$ strings [filename]`
- Determine the type of executable
 - ELF – 'Executable and Linkable Format': Linux program
 - PE – 'Portable Executable': Windows program
 - AIF – 'ARM Image Format': Embedded systems`$ file [filename]`
- Make it runnable (in Linux)
`$ chmod +x [filename]`
- Run the program to see what it does!
 - Do some analysis to see if you can 'beat' it w/out diving too deeply
- 'Fuzz' the program to see if you can make it fail un-gracefully
 - Enter data that the program isn't expecting



Reverse engineering – advanced challenges

- Packed executables: some programs can't be disassembled because they are 'packed', or compressed
 - Packing is used to make programs smaller to reduce hard drive and network overhead
 - Also used by malware authors to obscure code and make them harder to analyze
 - Analyst must let the 'unpacker' run, then stop the program to analyze
- Static or dynamic analysis
 - Static analysis – disassemble and analyze assembly-language code
 - Or, decompile and examine representation of original source code
 - Dynamic analysis – run program in debugger and examine and/or control the flow of execution



Challenge types: forensics

- Given a digital artifact, find some bit of information to answer a challenge question
 - Drive image
 - Partial file system
 - Memory image
 - Packet capture file
- Useful tools:
 - Autopsy – Linux tool for analyzing drive images
 - RegRipper – Linux tool for analyzing Windows registry
 - Volatility – Linux memory forensics tool
 - Rekall – Windows memory forensics tool (FireEye product)
 - Linux search tools
 - Find, grep, etc.



Challenge types: reconnaissance

- These problems focus on general problem-solving
 - Often not much 'cyber' experience needed
- Usually require competitors to follow a trail of clues to reach a final flag.
- Useful tools:
 - *Google and other search engines*
 - Internet Wayback Machine (archive.org)
 - Whois lookups? (whois.icann.org)
 - Shodan? (www.shodan.io)



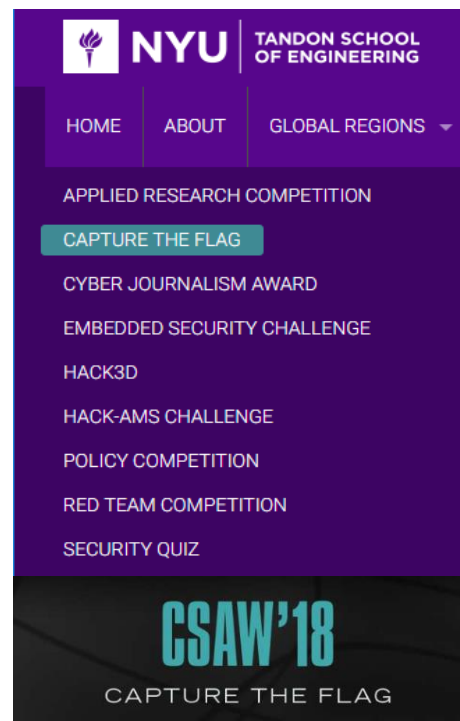
High school competitions

- picoCTF
 - Annual HS contest by Carnegie Mellon's CyLab and the CMU video game program
- EasyCTF
- HSCTF – “The first CTF by high schoolers, for high schoolers”
- RUSecure CTF
 - Radford University.
 - 3 rounds – preliminary round, qualifying round, in-person finals
- Cyberpatriot
 - Air Force sponsored team-based program



Collegiate/professional competitions

- CSAW CTF
 - Annual CTF hosted by NYU-Poly
 - Qualification round followed by in-person final
- Virginia Cyber Fusion CTF
 - Invitation-only event held at VMI for Governor's Cyber Cup
- DEF CON CTF
 - Gold standard of CTFs; held during annual DEF CON conference
- Collegiate Cyber Defense Competition (CCDC)
 - Annual inter-collegiate competition
 - 2018 CCDC champs: University of Virginia!
- LOTS more listed at <https://ctftime.org/>



VIRGINIA
CYBER RANGE

https://ctftime.org/

- Central repository of CTF information
 - World-wide leaderboard
 - Calendar of upcoming CTFs
 - CTF archive (going back to 2011)
 - CTF solution write-ups!

The screenshot shows the CTftime.org website interface. The top navigation bar includes the CTftime logo and links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, Contact us, and About. A 'Sign in' button is located on the right.

Team rating

2018 2017 2016 2015 2014 2013 2012 2011

Place	Team	Country	Rating
1	Dragon Sector	🇺🇸	666.773
2	Plaid Parliament of Pwning	🇺🇸	538.822
3	dcua	🇩🇪	510.212
4	TokyoWesterns	🇯🇵	485.811
5	p4	🇺🇸	461.567
6	LCeBC	🇩🇪	433.455
7	Bushwhackers	🇩🇪	411.255
8	CyKOR	🇰🇷	405.853
9	RPISEC	🇺🇸	316.613
10	0daysober	🇩🇪	316.574

[Full rating](#) | [Rating formula](#)

Past events

With scoreboard All

CODE BLUE CTF 2018 Quals

July 29, 2018 11:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points
1	Dragon Sector	🇺🇸	0.000*
2	CyKOR	🇰🇷	0.000
3	ISpamAndHex	🇩🇪	0.000

542 teams total | [Tasks and writeups](#)

ISITDTU CTF 2018 Quals

July 28, 2018 19:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points
1	Pinonymous	🇺🇸	0.000*
2	noraneco	🇯🇵	0.000
3	b0s	🇩🇪	0.000

320 teams total | [Tasks and writeups](#)

CTFZone 2018 Quals

July 22, 2018 21:00 UTC | On-line

Place	Team	Country	Points
1	LCeBC	🇩🇪	47.820
2	ISpamAndHex	🇩🇪	26.706

Upcoming events

Open

Format	Name	Date	Duration
📅	Hackcon 2018	Wed, Aug 15, 18:30	1d 0h
📅	On-line	— Thu, Aug 16, 18:30 UTC	31 teams



VIRGINIA
CYBER RANGE

Free CTF frameworks (host your own!)

- CTFd
 - The CTF you use today is based on this
 - Purely Jeopardy-style
 - Downloadable from GitHub
- *OR*
- Hosted at <https://ctfd.io>, starting at \$50/month
- Facebook CTF (fbctf)
 - Downloadable from GitHub
 - Install as Docker container
 - Three “levels”
 - Quiz levels – trivia questions
 - Flag levels – Jeopardy-style challenges
 - Base levels – ‘King of the Hill’



Questions?



VIRGINIA CYBER RANGE

Making Virginia a national resource for cybersecurity education.

CONNECT WITH US

@VaCyberRange

 [viriniacyberrange.org](https://twitter.com/VaCyberRange)



Virginia and Google Cloud

Your partner in security

Google Cloud

Agenda



Introductions
and Objectives



Infrastructure
Security



Account Security and
Phishing Protection



Data Loss
Protection



Questions

Your Google Team



Scott Fleming

Head of Professional
Services - Public Sector
and Security



Jennifer Whitty

Technical Account
Manager



Kate Johnson

Technical Account
Manager

Infrastructure Security

Google Cloud

Security Research

- Experimenting with Post-Quantum Cryptography
- Guided in-process fuzzing of Chrome components
 - 700 VMs, in 30 days - 14,366,371,459,772 unique test inputs
- Project Zero
 - Windows Kernel Fuzzing
 - How to Compromise the Enterprise Endpoint
 - Exploiting Recursion in the Linux Kernel
 - Flash Exploits
 - OS X and iOS Kernel Exploits
- Does Dropping USB Drives Really Work?
 - Yes, it does

Transparency, audits and certification

Proof at your fingertips and independent verification



Google security and compliance whitepaper

Contains detailed information on data usage, compliance, and a list of configurable features and settings that customers can use to enhance their security and data management practices



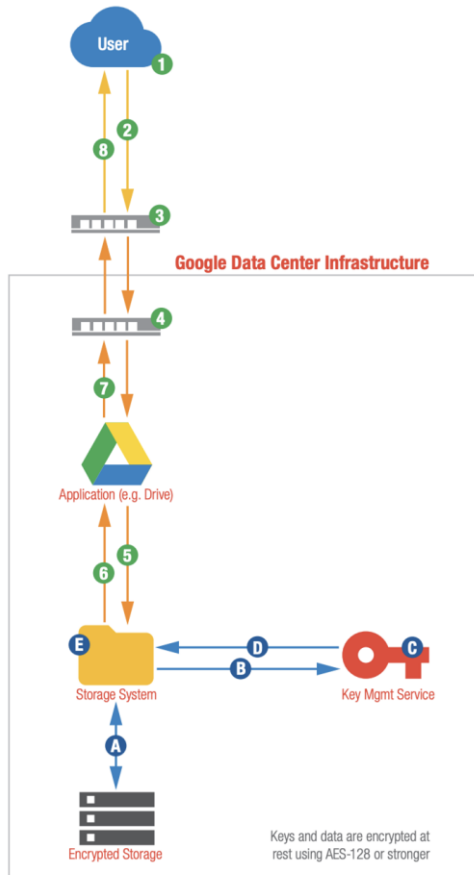
Google's IP data network consists of our own fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services across the globe

Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages

Google encryption whitepaper

Includes detailed information on Google's approach to encryption and how it keeps your sensitive information safe

- How Google approaches encryption
 - Encryption of data stored at rest
 - Data on disk
 - Key management and decryption process
 - Data on backup media
 - Encryption of data in transit
 - Data traveling over the Internet
 - Data moving between data centers

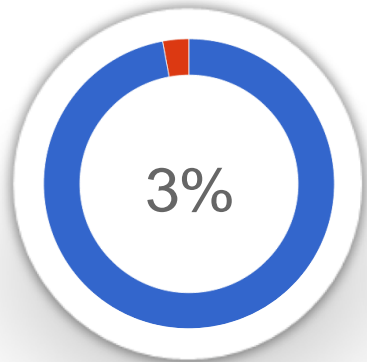


Account Security and Phishing Protection

Google Cloud

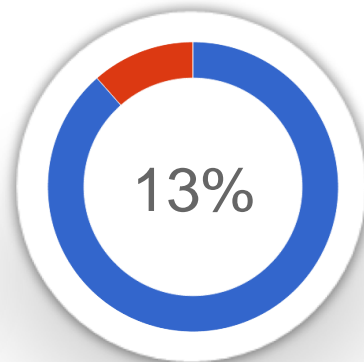
Is phishing effective?

The **most obvious** phishing webpages



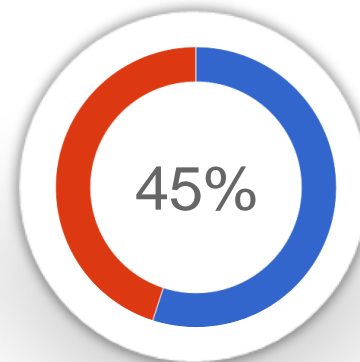
Trick users
3%
of the time

Average phishing webpages



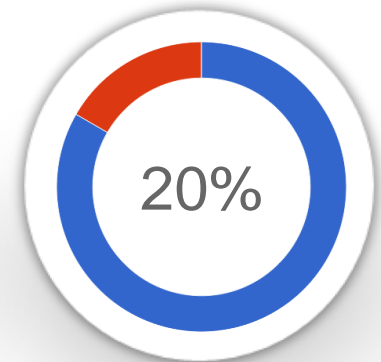
Trick users
13%
of the time

The **most believable** phishing webpages



Trick users
45%
of the time

Hijackers **move fast**



20% of accounts are
accessed within
30 minutes
of being phished

[Data Source](#)

56%

priced their credentials at over \$1,000. Others, however, were willing to go as low as \$100

42%

could continue to access their accounts and data after leaving the company

Selling Passwords?

32%

shared passwords with co-workers

27%

of office workers in the US (20% globally) would sell their passwords

Mandatory Password Changes

- University of North Carolina at Chapel Hill study of 10,000 defunct accounts
- Used sequences of 4 to 15 of the user's previous passwords – 51,141 passwords in all
- For 7,752 accounts, the researchers were able to crack at least one password that was not the last password the user created for that account.

For 17% of the accounts they studied, knowing a user's previous password allowed them to guess their next password in fewer than 5 guesses

Humans and passwords

Passwords are no longer enough

- Nearly 75% of users use shared passwords
- Additional verification methods, such as 2-Factor Authentication, must be implemented

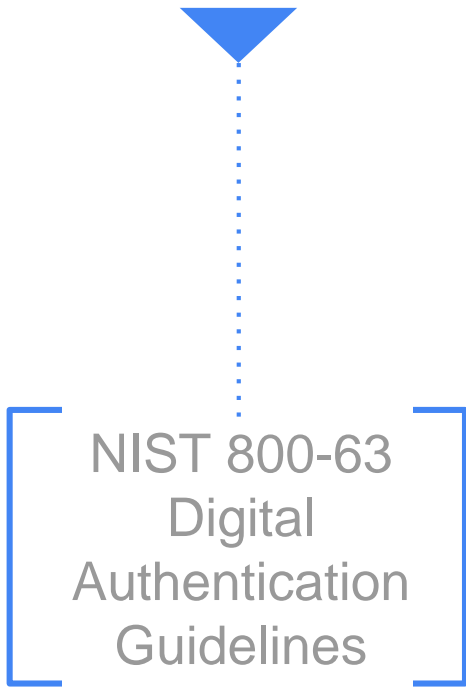
Frequent password change policy

- Users select weak passwords
- Change passwords to predictable ways

Password recovery policy

- Can be your weakest link if the recovery process is not properly protected



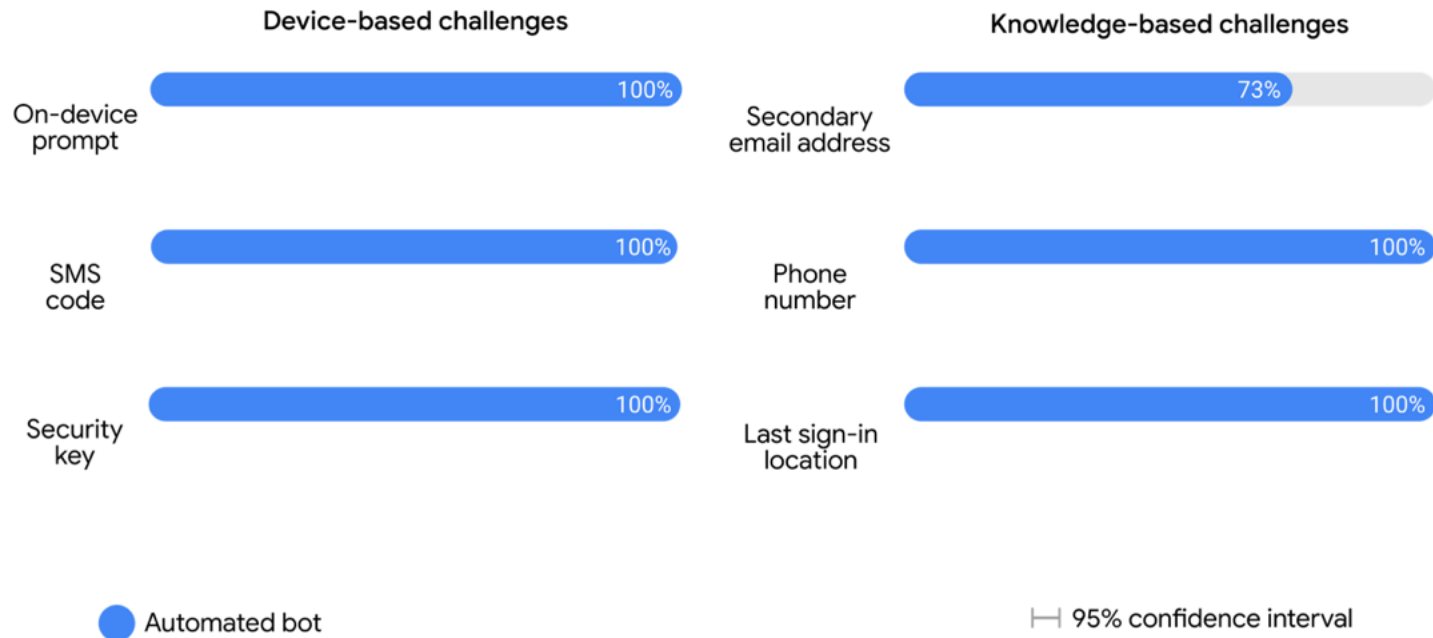


NIST 800-63
Digital
Authentication
Guidelines

- 1 “Memorized secrets SHALL be at least 8 characters in length ... Some values ... may be disallowed based on their appearance on a blacklist of compromised values. No other complexity requirements for memorized secrets are imposed.”
- 2 “OOB (Out of Band, aka OTP) using SMS is deprecated, and may no longer be allowed”
- 3 “Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically) unless there is evidence of compromise”

What types of attacks are you facing?

Account takeover prevention rates by challenge type



What types of attacks are you facing?

Account takeover prevention rates by challenge type



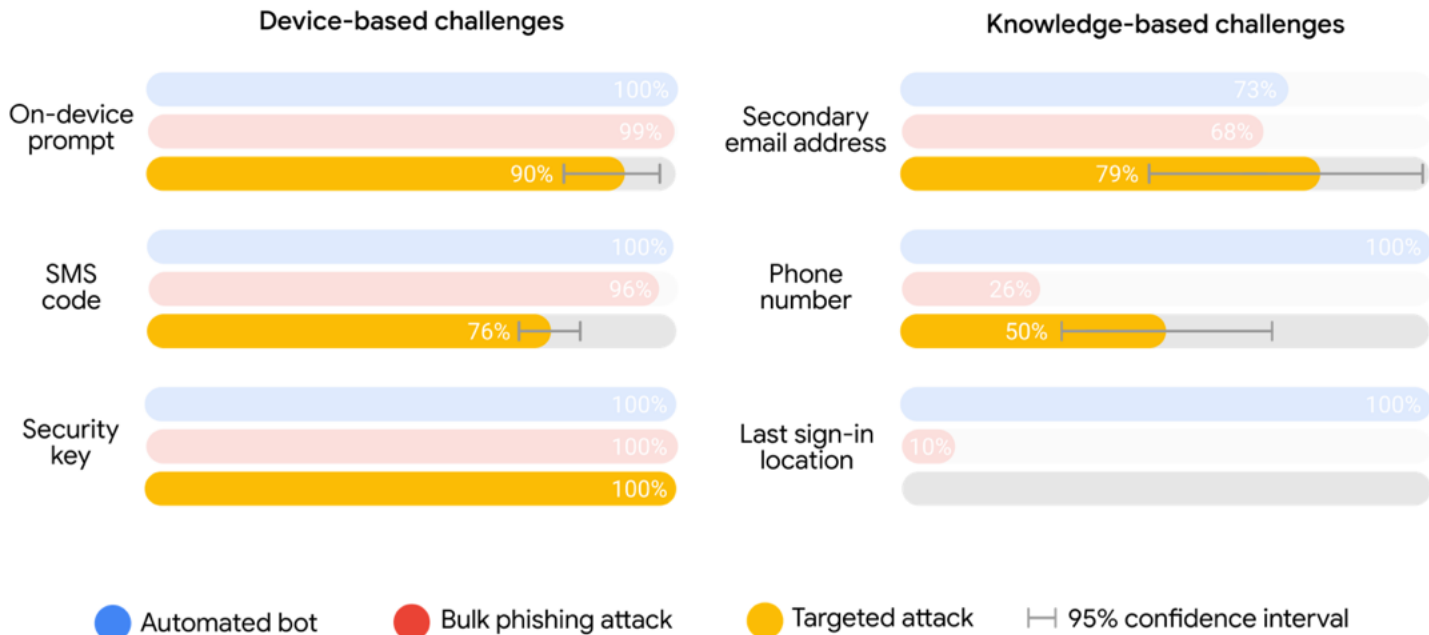
What types of attacks are you facing?

Account takeover prevention rates by challenge type



What types of attacks are you facing?

Account takeover prevention rates by challenge type



2-Step verification and security keys



Google Titan Security Key



Yubico Security Key

Universal second-factor security keys

Security Keys are second-factor devices that protect users against phishing and man-in-the-middle attacks.

Strong security

- Phishing—Uses cryptographic assertions
- Man-in-the-Middle—Binds cryptographic assertions to website origin and properties of the TLS connection

Easy for users

- Effortless, easy-to-learn, and infrequent errors
- Total authentication time decreased significantly using Security Keys vs other models

Open standard

- Standardized within the the FIDO Alliance organization as the [Universal Second Factor \(U2F\)](#)
- Used internally at Google with over 50,000 users



Security keys improve user experience

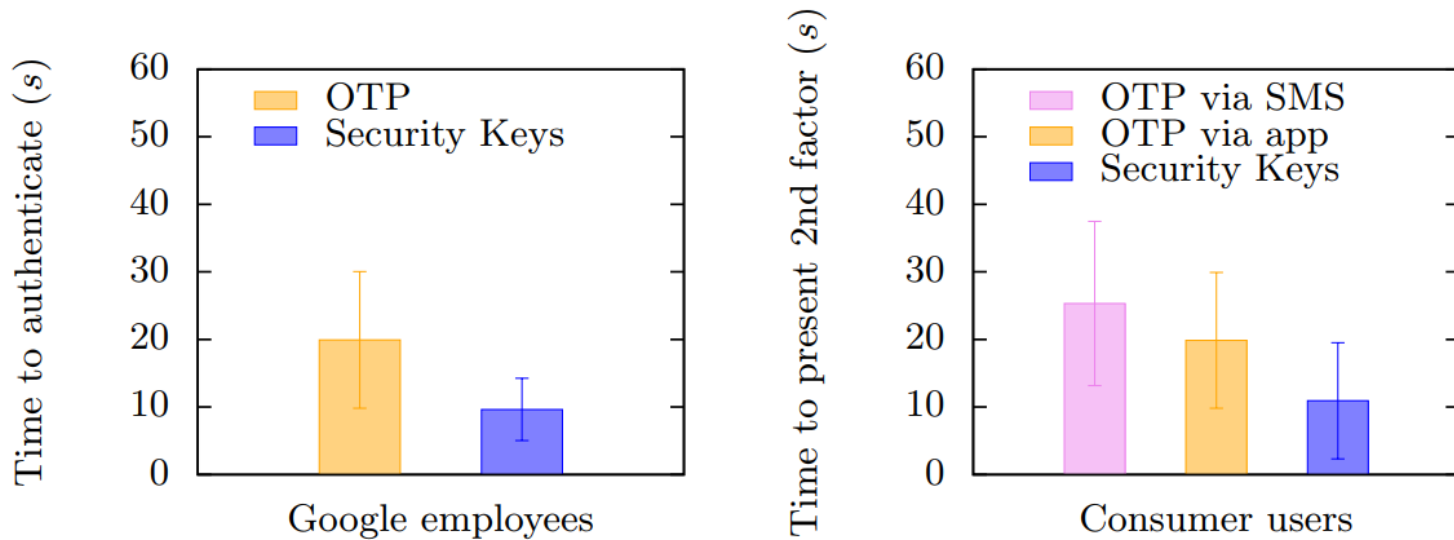


Fig. 6: Time spent authenticating

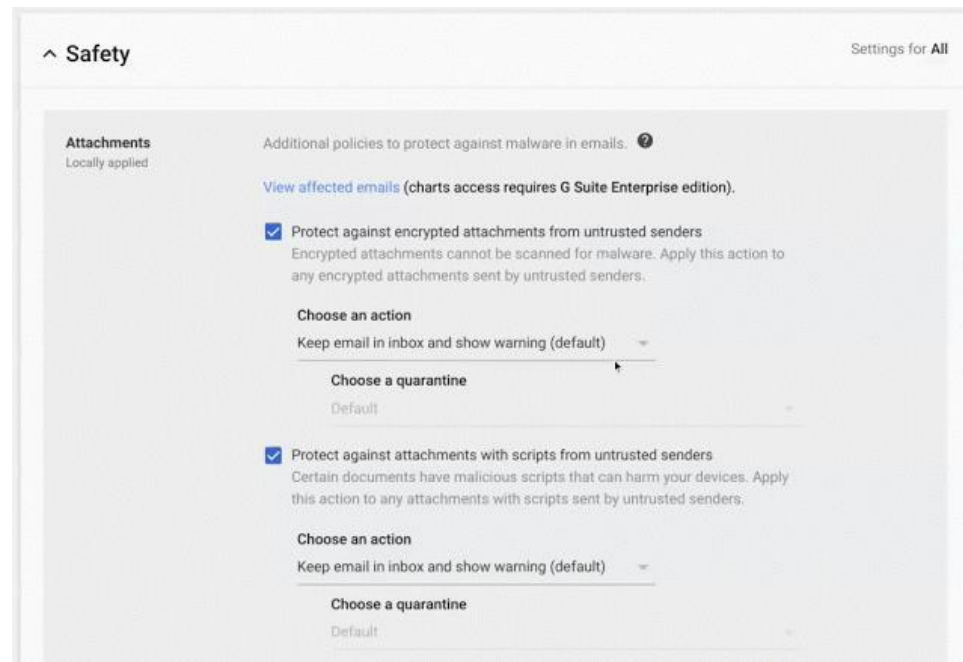
[*Data Source](#)

Advanced phishing and malware protection for Gmail (BETA)

We're launching a beta program to provide admins with even more controls for advanced anti-phishing and malware protections via the advanced safety settings in Gmail.

Admins will have new controls to:

- Place emails into a quarantine
- Protect against anomalous attachment types in emails
- Protect your Google Groups from inbound emails spoofing your domain



[Blog post](#) - [Documentation](#)

Control G Suite access with context-aware access (BETA)

Context-aware access allow G Suite admins to dynamically control access to G Suite apps based on a user's identity and the context of their request (device security status, IP address, etc.), allowing admins to

- Set up different access levels based on a user's identity and context of the request.,
- Use granular controls for different organizational units (OU)
- Control access to several G Suite apps by setting different policies for the different access level profiles that have been set up

The screenshot displays the Google Admin console interface for configuring context-aware access. On the left, a panel titled 'Login from corporate devices' includes an 'EDIT INFO' button. The main area is titled 'Access level conditions' and features a toggle for 'A user gets access if they:'. The 'Meet these conditions' option is selected. Below this, several policy settings are visible: 'Device policy' (dropdown), 'Device password required' (Yes), 'Device encryption' (dropdown), 'Windows policy' (Optional. Minimum version in semantic versioning format: MAJOR.MINOR.PATCH.), 'macOS policy' (Optional. Minimum version in semantic versioning format: MAJOR.MINOR.PATCH.), 'ChromeOS policy' (Optional. Minimum Platform version in semantic versioning format: MAJOR.MINOR.PATCH. with a 'Learn more' link), 'Verified Chrome OS' (Not required), and 'Corporate Owned Device' (Required).

[Blog post - Documentation](#)

Advanced protection program

For users you identify as most at risk to be targeted

[Blog Post](#)

Data loss prevention and protection in Google

Google Cloud

^4[0-9]{12}(?:[0-9]{3})?\$
^5[1-5][0-9]{14}\$
^3[47][0-9]{13}\$
^389[0-9]{11}\$
^3(?:0[0-5]||[68][0-9])[0-9]{11}\$
^65[4-9][0-9]{13}|64[4-9][0-9]{13}|6011[0-9]{12}|(622(?:12[6-9]|1[3-9][0-9]||[2-8][0-9][0-9]|9[01][0-9]|92[0-5])[0-9]{10})\$
^(?:2131|1800|35\d{3})\d{11}\$
^(?:4[0-9]{12}(?:[0-9]{3})?|5[1-5][0-9]{14})\$
^63[7-9][0-9]{13}\$
^(6304|6706|6709|6771)[0-9]{12,15}\$
^(5018|5020|5038|6304|6759|6761|6763)[0-9]{8,15}\$
^(6334|6767)[0-9]{12}|(6334|6767)[0-9]{14}|(6334|6767)[0-9]{15}\$
^(4903|4905|4911|4936|6333|6759)[0-9]{12}|(4903|4905|4911|4936|6333|6759)[0-9]{14}|(4903|4905|4911|4936|6333|6759)[0-9]{15}|564182[0-9]{10}|564182[0-9]{12}|564182[0-9]{13}|633110[0-9]{10}|633110[0-9]{12}|633110[0-9]{13})\$
^62[0-9]{14,17})\$
^9[0-9]{15}\$
^(6541|6556)[0-9]{12}\$

Data loss prevention for Gmail

Prevents data leakage

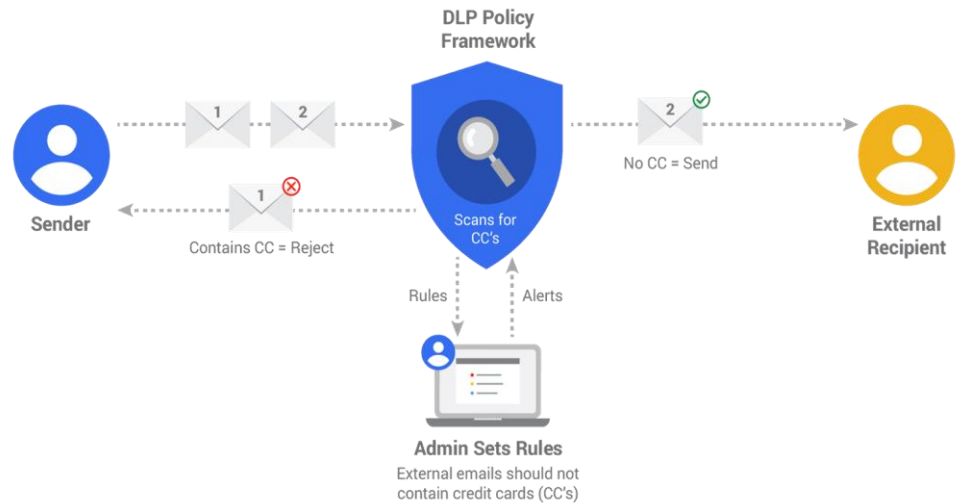
- Scans outbound email traffic for sensitive data, such as credit card, social security numbers, or custom rules

Predefined content detectors

- Covers personally identifiable information (PII) in several countries and HIPAA data
- Custom content detectors using regex
- Content detection thresholds
- Specify appropriate action

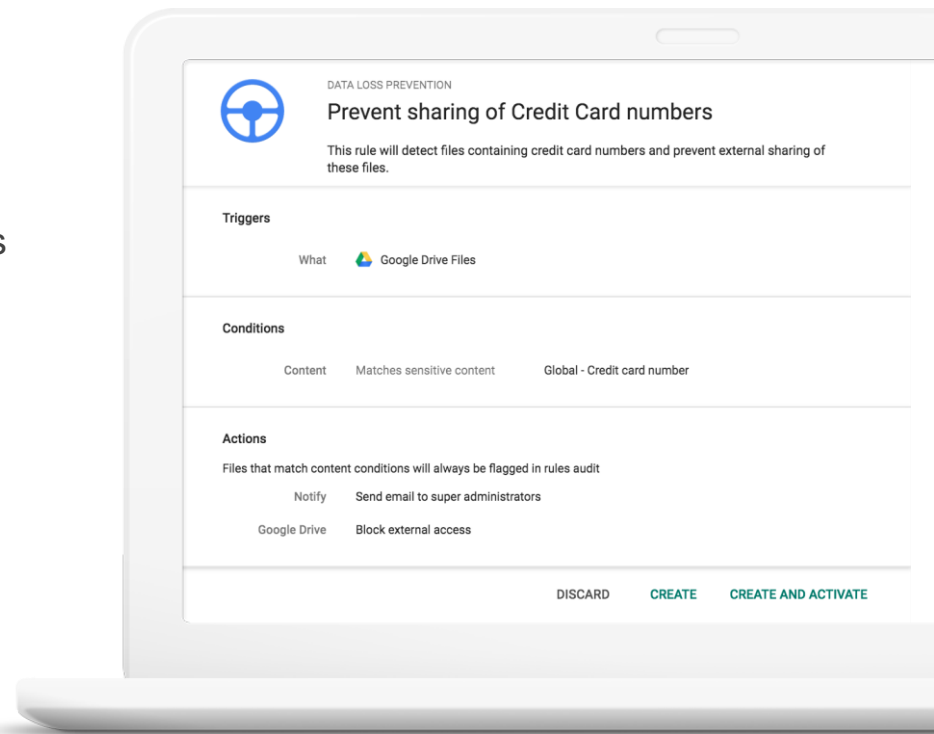
Attachment scanning

- Documents, presentations, spreadsheets



Protect sensitive information with DLP

- DLP for Gmail and Drive
- Easy to deploy with predefined content detectors
- 50+ Global content types
- Custom rules
- Optical Character Recognition
- Content thresholds

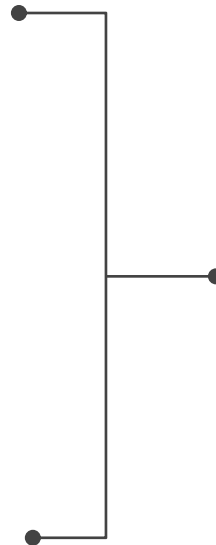


Easy to deploy: global content detectors

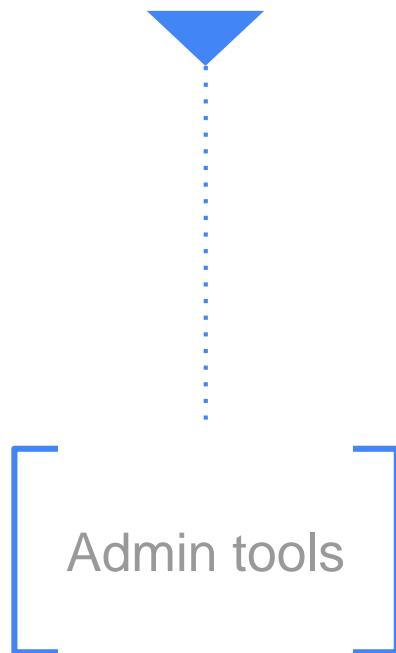


First party apps are well protected

- Drive data loss prevention
- Gmail data loss prevention
- Drive OU-based sharing settings
- Drive IRM support
- Drive expiring access
- S/MIME encryption for Gmail
- Secure sandboxing



But what about data breaches through 3rd party apps?



Helping your users remain secure

- 1 Alerts - Understand what is happening in your domain
- 2 Email Security (SPF/DKIM/DMARC) - protect your users and constituents from a malicious actor pretending to be you.
- 3 Have an incident response plan!

Alerting

Rules

Name	Status	Actions	Alerts
Device compromised Provides details about devices in your domain that have entered a compromised state.	Active	Send Notification	On
Domain data export initiated A super administrator for your Google account has started exporting data from your d...	Active	Send Notification	On
Google Operations Provides details about security and privacy issues that affect your G Suite services.	Active	Send Notification	On
Government-backed attacks Warnings about potential government-backed attacks.	Active	Send Notification	On
Leaked password Google detected compromised credentials requiring a reset of the user's password.	Active	Send Notification	On
Malware message detected post-delivery Messages detected as malware post-delivery that are automatically reclassified.	Active	Send Notification	On
Phishing in inboxes due to bad whitelist Messages classified as spam by Gmail filters delivered to user inboxes due to whitelist...	Active	Send Notification	On
Phishing message detected post-delivery Messages detected as phishing post-delivery that are automatically reclassified.	Active	Send Notification	On
Spike in user-reported spam An unusually high volume of messages from a sender that users have marked as spam.	Active	Send Notification	On
Suspicious device activity Provides details if device properties such as device ID, serial number, type of device, or...	Active	Send Notification	On

Reporting and audit in the admin console

Domain level reports:

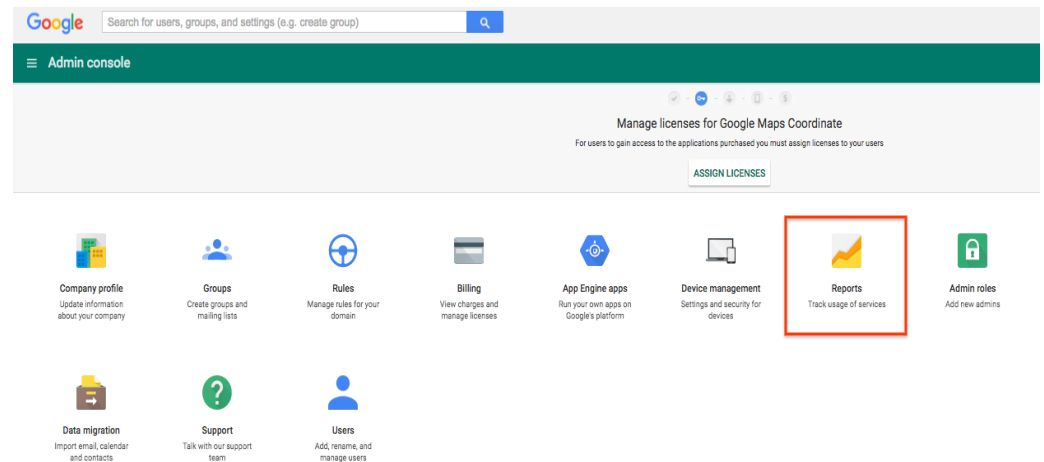
- Highlights page
- Aggregate reports: accounts, Gmail, Drive, Chrome, Mobile, Hangouts

User level reports:

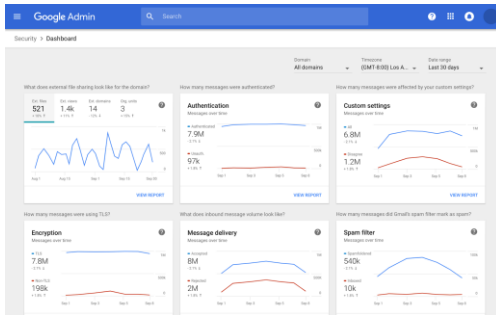
- Apps usage
- Security
- Accounts reports

Audit reports:

- Directory: Admin, Login, Oauth Tokens
- Apps: Gmail, Drive, Calendar, Groups
- Devices: Mobile

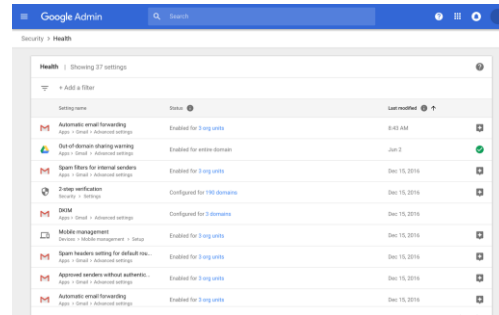


G Suite security center



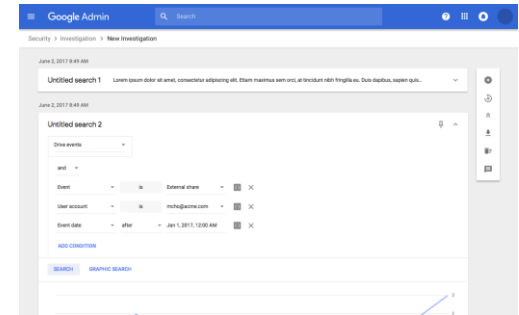
Security dashboards

Provide admins and IT decision makers with actionable security insights (e.g. phishing risks)



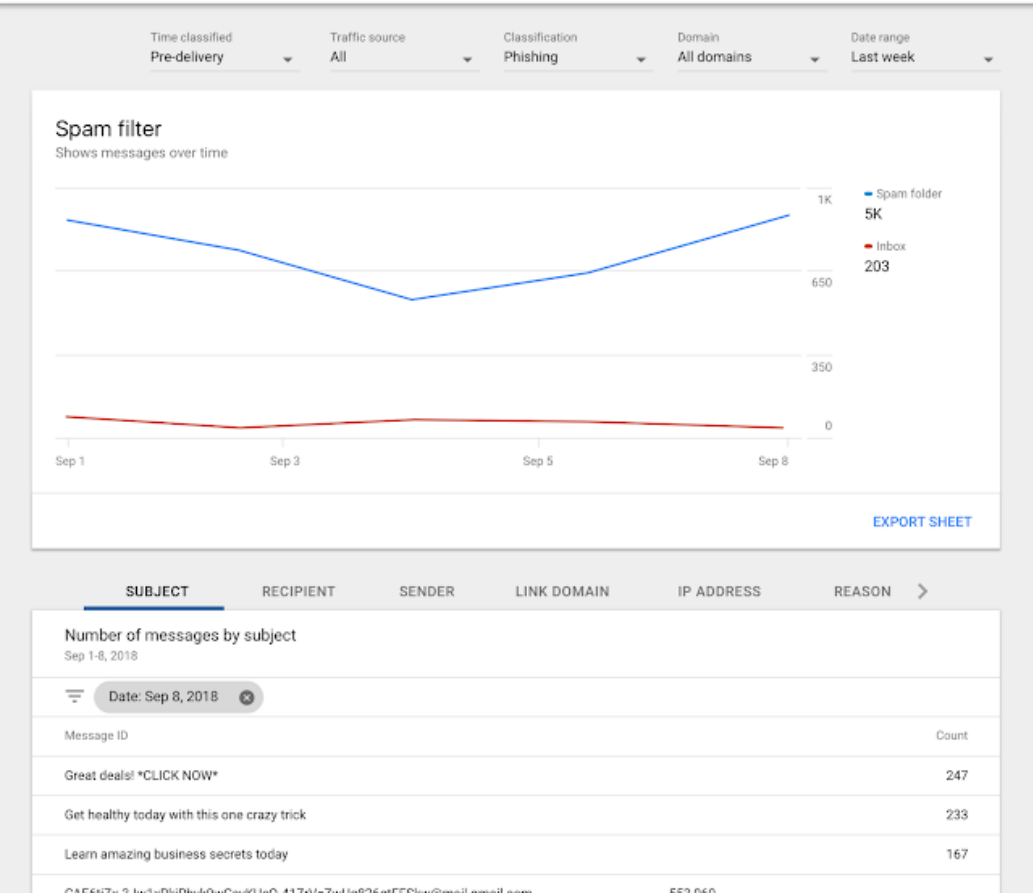
Security health

Help admins manage and improve the security posture of their domain (e.g. proactive phishing protection)



Threat intelligence

Investigation and remediation: help admins diagnose, triage and **resolve** security issues across G Suite. **Incident detection and alerts**



Health | Showing 37 settings

+ Add a filter

Setting name	Status	
Automatic email forwarding Apps > Gmail > Advanced settings	Enabled for 3 org units	+ [Recommendation]
Out-of-domain sharing warning Apps > Gmail > Advanced settings	Enabled for entire domain	+ [Checkmark]
Spam filters for internal senders Apps > Gmail > Advanced settings	Enabled for 3 org units	+ [Checkmark]
2-step verification Security > Settings	Configured for 190 domains	+ [Checkmark]
DKIM Apps > Gmail > Advanced settings	Configured for 3 domains	+ [Checkmark]
Mobile management Devices > Mobile management > Setup	Enabled for 3 org units	+ [Checkmark]
Spam headers setting for default rou... Apps > Gmail > Advanced settings	Enabled for 3 org units	+ [Checkmark]
MX record Apps > Gmail > Advanced settings	Configured for all domains	+ [Checkmark]
Approved senders without authentication Apps > Gmail > Advanced settings	Enabled for 3 org units	+ [Checkmark]
Automatic email forwarding Apps > Gmail > Advanced settings	Enabled for 3 org units	+ [Checkmark]

Recommendation

When you disable the automatic forwarding option, it reduces your risk of data exfiltration through email forwarding. When this setting is disabled, your users won't see the option in their Gmail settings, and any existing user-created forwarding rules or filters no longer result in forwarded messages. Admin created forwarding rules would still apply to those users.

[LEARN MORE](#)

Secure configuration

You've configured your MX records to point to Google's mail servers as the highest priority record to ensure correct mail flow to your G Suite domain users. This reduces the risk of [data deletion](#) (through lost email) and [malware](#) threats.

[LEARN MORE](#)

Gmail logs in BigQuery

```
SELECT FORMAT_UTC_USEC(event_info.timestamp_usec) as timestamp,  
       message_info.subject,  
       message_info.source.address,  
       message_info.destination.address,  
       message_info.rfc2822_message_id  
FROM (FLATTEN([your_dataset_id.daily_YYYYMMDD], message_info.destination.address))  
WHERE  
       message_info.triggered_rule_info.consequence.action == 17  
       and message_info.destination.address == "recipient@example.com"  
LIMIT 1000
```

```
SELECT EXACT_COUNT_DISTINCT(message_info.rfc2822_message_id)  
FROM [your_dataset_id.daily_YYYYMMDD]  
WHERE message_info.destination.address == "recipient@example.com"
```

Questions

Google Cloud

Thank you.

Please direct follow up questions to
commonwealthofvirginia@google.com

Google Cloud



Virginia Information Technologies Agency

Upcoming Events





ISC2 Richmond presents RVAbc

- ISC2 is presenting RVAbc
 - **Richmond Blockchain Technology Conference**
 - Oct. 18, 2019
 - Hilton Richmond Downtown
 - Visit: <https://www.rvabc.capital/> for details
 - RVAbc is currently looking for speakers as well as sponsors



ISACA Virginia chapter

The ISACA Virginia chapter

Next monthly lunch meeting:

Sept. 12, 2019

11:30 a.m. to 1 p.m.

Speaker: Charlene Watson

Topic: COBIT 2019

Where: Delta Hotel, Richmond

Contact Chandra Barnes for add'l info



VASCAN conference

Virginia Alliance for
Secure Computing and Networking

Oct. 8-9, 2019
Hotel Madison and
Shenandoah Valley Conference Center
Harrisonburg, VA
<http://vascan.org/>



VASCAN founders award

The Virginia Alliance for Security Computing and Networking (VASCAN) is soliciting nominations for the **2019 VASCAN Founders Award** (Formerly the Shirley Payne IT Security Advancement Award).

Send your nominations to Doug Streit at ODU
jstreit@odu.edu

If you need a nominating form, contact CSRM



IS orientations

Current schedule:

- Sept. 26 1-3 p.m.
- Dec. 10 1-3 p.m.

Link for registration:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



IS Orientation

September 26, 2019

1:00p – 3:00p

Room 1221

December 10, 2019

1:00p – 3:00p

Room 1221

Register @:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



VLGAA fall conference

The Virginia Local Government Auditors Association (VLGAA) fall conference

Date: Sept. 20, 2019

Location: The Place at Innsbrook

Event and registration information can be found at:
<https://s01.123signup.com/Member?PG=1538610182400&P=15386101362903141433801100&Info=>

Earn up to 8 CPE's



Cybersecurity Awareness Month

OWN
SECURE
PROTECT

IT.

OCTOBER 2019
National Cybersecurity
Awareness Month
#BeCyberSmart





Category – own it

Own it: understand your digital profile

Potential topics:

- Privacy settings
- Safe social media posting
- Bring your own device (BYOD)
- Internet of Things/Smart technology
- Don't let your tech own you

Category – protect it

Protect it - maintain your digital profile

Potential topics:

- Researching and assessing your digital profile
- “Cyber hygiene”
- Physical security and cybersecurity comparison

Category – secure it

Secure IT - secure your digital profile

Potential topics:

- Creating strong passwords
- Multifactor authentication
- Ecommerce
- Zero trust
- Protecting against phishing



Resources

- National Initiative for Cybersecurity Careers and Studies
- <https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019>
- Toolkit
- https://niccs.us-cert.gov/sites/default/files/documents/pdf/dhs_ncsam2019_toolkit_508c.pdf?trackDocs=dhs_ncsam2019_toolkit_508c.pdf
- Speaker form
- <https://niccs.us-cert.gov/sites/default/files/documents/pdf/cisa%20ncsam%202019%20speaker%20request%20form.pdf?trackDocs=cisa%20ncsam%202019%20speaker%20request%20form.pdf>
- DHS
- <https://www.dhs.gov/national-cyber-securityawareness-month>
- Stay safe online
- <https://staysafeonline.org/ncsam>



What you can do now

Order materials from the FTC promoting online safety

Start promoting NCSAM via social media, press releases and your agency website

Plan activities for employees to participate in

Get your leadership involved....



Future ISOAG

Mandatory meeting

Oct. 2, 2019 @ CESC 1-4 p.m.

**Speakers:, Capture the flag event
VITA staff**

ISOAG meets the first Wed. of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

