How The United States Protects Citizens From State Actors

Joey Whitmore

Cyber 280

Joey Whitmore

4/01/2023

Introduction

In the modern digital age, the internet has become an integral part of our lives, and the United States government takes the online safety of its citizens very seriously. The US government works tirelessly to protect its citizens from various online threats, including foreign cyber attackers who pose a risk to national security and individual privacy.

To ensure online safety, the US government has implemented various measures and initiatives to detect, prevent, and respond to cyber attacks. One of the primary ways the government ensures online safety is by investing in cybersecurity research and development to improve the country's cyber defenses. The government also partners with private organizations, academia, and international bodies to develop new strategies and technologies to counter cyber threats. Also the extensive use of VPNS, Cyber policies, and their own DHS policies help reduce cyber threats.

Additionally, the US government has established a dedicated cybersecurity agency, the Cybersecurity and Infrastructure Security Agency (CISA), to protect critical infrastructure and respond to cyber threats (About CISA | CISA, n.d.). CISA collaborates with other government agencies, private entities, and international partners to enhance the country's cybersecurity posture.

Despite these efforts, citizens must take individual responsibility to protect themselves from foreign cyber attackers. There are several ways citizens can safeguard their online activity and prevent foreign attackers from gaining unauthorized access to their personal data. One of the most important steps is to use strong and unique passwords for all online accounts and avoid reusing passwords across multiple accounts. Citizens should also enable two-factor authentication whenever possible to add an extra layer of protection to their accounts.

Another essential step in protecting oneself from foreign cyber attackers is to remain vigilant and avoid falling victim to phishing scams. Phishing is a tactic used by attackers to steal sensitive information, such as login credentials or financial information, by posing as a legitimate entity. Citizens should avoid clicking on suspicious links or opening unsolicited emails and messages.

Overview of the Research

The internet has become an essential component of our modern lives, and the government of the United States takes online safety very seriously. The United States government puts in a lot of effort to keep its citizens safe online from a variety of threats, including foreign cyber attackers who can harm national security and privacy.

The United States government has implemented a number of initiatives to detect, prevent, and respond to cyberattacks in order to guarantee online safety. Investing in cybersecurity research and development in order to enhance the nation's cyber defenses is one of the primary ways that the government ensures online safety. The public authority likewise cooperates with private associations, the scholarly world, and global bodies to foster new methodologies and advances to counter digital dangers. Cyber policies, their own DHS policies, and the widespread use of virtual private networks (VPNs) all contribute to the reduction of cyber threats.

Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) has been established by the US government to safeguard critical infrastructure and respond to cyber threats (About CISA | CISA, n.d.). To improve the nation's cybersecurity posture, CISA works with other government agencies, private organizations, and international partners.

In spite of these efforts, citizens must take individual responsibility for safeguarding themselves against cyberattackers from outside the country. Citizens can protect their online activities and prevent foreign attackers from gaining access to their personal data in a number of different ways. Utilizing strong, one-of-a-kind passwords for all online accounts and avoiding password reuse across multiple accounts is one of the most crucial steps. To further safeguard their accounts, citizens should also, whenever possible, enable two-factor authentication.

Maintaining vigilance and avoiding phishing scams is an additional crucial step in defending against foreign cyber attackers. Attackers use phishing to pretend to be a legitimate entity in order to steal sensitive information, such as login credentials or financial information. Residents ought to abstain from tapping on dubious connections or opening spontaneous messages and messages.

The VPN client on a user's device establishes a secure connection to a VPN server when the user connects to a VPN. This association is scrambled utilizing progressed encryption conventions, like AES (High level Encryption Standard) or SSL (Secure Attachment Layer). All data sent between the user's device and the VPN server is encrypted to prevent any potential interceptors from reading it.

All internet traffic from the user's device is routed through the VPN server once it is connected to it. Encrypting all traffic that is sent between the user's device and the internet is performed by the VPN server, which acts as a middleman. This means that the encrypted data that is being sent from the user's device to the VPN server cannot be read by anyone even if they were to intercept it.

As well as scrambling web traffic, VPNs additionally utilize other safety efforts to guarantee that client information stays private and secure. For instance, numerous VPNs utilize an interaction called burrowing, which makes a safe passage through which information is sent between the client's gadget and the VPN server(Norton, What is A VPN?). Encryption ensures that no one can intercept data sent between the two sides of this tunnel.

Additionally, VPNs make use of a variety of authentication and authorization methods to guarantee that the VPN can only be accessed by authorized users. For instance, in order to log in to a lot of VPN services, users are required to enter a username and password. Some VPNs likewise expect clients to enter a two-factor verification code, which gives an extra layer of safety (Norton,What is a VPN?).

At last, it is actually quite important that not all VPNs are made equivalent as far as their encryption and safety efforts. Some VPNs might utilize more fragile encryption conventions, or might not have strong verification and approval components set up. Users should do their research and choose a VPN provider with a good reputation for privacy and security. They should also make sure that their VPN client is set up correctly to give them the best encryption and security.

Organizations can manage and reduce cybersecurity risk with the help of the NIST Cybersecurity Framework's guidelines, best practices, and standards. The structure is broadly taken on by government offices, confidential area associations, and different substances as a device for further developing network safety act. The framework is compatible with other global cybersecurity frameworks and guidelines and is designed to be adaptable.

Different wellsprings of network protection rules and principles that are pertinent to the US incorporate the Worldwide Association for Normalization (ISO) and the Global Electrotechnical Commission (IEC). For information security management systems (ISMS), these organizations offer a set of guidelines that can be used to put together an efficient cybersecurity program.

In addition, cybersecurity best practices and guidelines are provided by the Center for Internet Security (CIS). A set of twenty security measures known as the CIS Controls can be utilized to lessen the likelihood of cyberattacks. The controls are mapped to various other cybersecurity frameworks, such as the NIST Cybersecurity Framework, and they are regularly updated to take into account shifting threat landscapes.

The Installment Card Industry Information Security Standard (PCI DSS) is a bunch of rules for associations that handle Visa information. The Payment Card Industry Security Standards Council (PCI SSC), which is made up of major credit card companies like Visa and Mastercard, is in charge of maintaining the standard. The standard specifies requirements for protecting cardholder information and ensuring the safety of payment systems.

The CISA Network safety Structure is an intentional system that is intended to be adaptable and versatile, and it is expected for use by associations of all sizes and types. The following are the five main functions of the framework: Protect, Identify, Identify, Respond, and Recover The framework's guidelines and best practices are based on these functions, which give a high-level view of the cybersecurity risk management process.

Understanding and managing cybersecurity risks to systems, assets, data, and capabilities is the primary focus of the first core function, Identify. Establishing risk management procedures and gaining an understanding of the cybersecurity environment are all part of this. Asset management, risk assessment, and governance are all parts of the Identify function.

Protect, the second core function, focuses on putting safeguards in place to safeguard crucial assets from cyber threats. This incorporates exercises, for example, access control, mindfulness and preparing, and information security. The Protect function is intended to safeguard critical assets' confidentiality, integrity, and availability while also lowering the likelihood of cyberattacks.

The goal of the third core function, Detect, is to find cybersecurity incidents that could harm important assets. This incorporates exercises like ceaseless checking, danger discovery, and abnormality location. The purpose of the Detect function is to enable prompt detection of cybersecurity events so that businesses can take appropriate measures to lessen their impact.

Respond, the fourth core function, focuses on responding to detected cybersecurity events. Planning for business continuity, disaster recovery, and incident response are all examples of this. The Answer capability is intended to limit the effect of network safety occasions on basic resources and to guarantee the association can rapidly recuperate from these occasions.

The fifth and last center capability, Recuperate, is centered around reestablishing capacities or administrations that have been hindered because of a network safety occasion. This incorporates exercises, for example, recuperation arranging, further developing flexibility, and speaking with partners. After a cybersecurity incident, the Recover function is intended to guarantee that businesses can quickly restore essential services and assets.

Notwithstanding these center capabilities, the CISA Network protection Structure incorporates a bunch of classes and subcategories that give more unambiguous direction on the most proficient method to carry out the system's rules and best practices. The tiers in which the categories and subcategories are arranged correspond to the organization's maturity level in cybersecurity risk management.

While Tier 2 organizations have established processes but have not yet fully implemented the framework's guidelines and best practices, Tier 1 organizations have informal or ad hoc cybersecurity risk management processes. Level 3 associations have executed the system's rules and best practices generally, while Level 4 associations have carried out the structure's rules and best practices in an exhaustive and proactive way.

The framework can be used to evaluate an organization's cybersecurity risk management maturity and identify areas for growth. Additionally, the framework can be utilized to demonstrate compliance with cybersecurity regulations and standards and to communicate cybersecurity risk management practices and priorities to stakeholders.

The CISA Cybersecurity Framework is a valuable resource for organizations that want to improve their cybersecurity posture and reduce the risk of cyber attacks. By following the framework's guidelines and best practices, organizations can establish a comprehensive and effective cybersecurity risk management program that is tailored to their specific needs and priorities. While the framework is voluntary, it is widely adopted by government agencies, private sector organizations, and other entities as a tool for improving cybersecurity posture and reducing cybersecurity risk.

DHS's cybersecurity policies are designed to be flexible and adaptable, and they are intended for use by government agencies, private sector organizations, and other entities. The agency has developed a range of policies and initiatives that are focused on identifying and managing cybersecurity risks, protecting critical infrastructure and information systems, detecting and responding to cyber threats, and promoting cybersecurity awareness and education.

One of DHS's key cybersecurity policies is the National Cybersecurity and Communications Integration Center (NCCIC), which serves as a 24/7 cyber situational awareness, incident response, and management center. The NCCIC is responsible for coordinating cybersecurity efforts across government agencies and private sector organizations, and it provides real-time information and analysis on cyber threats and incidents.

Another important DHS cybersecurity policy is the Critical Infrastructure Cyber Community (C3) Voluntary Program, which is designed to help critical infrastructure owners and operators manage cybersecurity risks. The C3 Voluntary Program provides a range of resources, including cybersecurity assessments, information sharing, and training, to help organizations improve their cybersecurity posture and reduce the risk of cyber attacks.

DHS has also developed the Cybersecurity and Infrastructure Security Agency (CISA), which is responsible for protecting the nation's critical infrastructure from cyber threats. CISA provides a range of services and resources to government agencies, private sector organizations, and other entities, including risk assessments, vulnerability scanning, incident response, and best practices guidance.

DHS has also developed a range of initiatives and programs to promote cybersecurity awareness and education. These include the Stop.Think.Connect. campaign, which is designed to educate the public about cybersecurity risks and best practices, and the Cybersecurity Education and Awareness Program (CEAP), which provides resources and training to government agencies and private sector organizations to improve cybersecurity awareness and education.

Overall, DHS's cybersecurity policies are designed to provide a comprehensive and coordinated approach to managing cybersecurity risks and protecting critical infrastructure and information systems. The agency's initiatives and programs are tailored to meet the needs of different entities and are focused on promoting collaboration, information sharing, and best practices adoption.

By following DHS's cybersecurity policies and initiatives, government agencies, private sector organizations, and other entities can improve their cybersecurity posture and reduce the risk of cyber attacks. The agency's policies are also designed to promote cybersecurity awareness and education, which is critical for building a culture of cybersecurity across the country.

Frameworks/Process

NIST Framework process:

Identify:

To manage cybersecurity risk to systems, people, assets, data, and capabilities, develop organizational understanding.
Effective usage of the Identify Function depends on the activities in that function.

Framework. An organization can concentrate and prioritize its efforts in accordance with its risk management strategy and business requirements by having a thorough understanding of the business context, the resources supporting important functions, and the associated cybersecurity risks.
Asset management, the business environment, governance, risk assessment, and risk management strategy are a few examples of result categories within this function.

Protect:

Create and put into place the necessary protections to guarantee the delivery of essential services.

A possible cybersecurity event's impact can be limited or contained with the help of the Protect Function. Identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology are a few examples of outcome categories within this function.

Detect:

Create and put into action the necessary activities to detect a cybersecurity event.
The Detect Function makes cybersecurity events quickly discoverable. Anomalies and Events, Security Continuous Monitoring, and Detection Processes are a few examples of result Categories under this function.

Respond:

Create and implement the necessary actions to respond to an identified cybersecurity incident.
The capacity to reduce the impact of a possible cybersecurity event is supported by the Respond Function. Response planning, communications, analysis, mitigation, and improvements are a few examples of result categories within this function.

Recover:

Create and put into action the necessary actions to maintain resilience plans and to restore any capabilities or services that were damaged as a result of a cybersecurity event.
The Recover Function encourages prompt return to routine operations in order to lessen the effects of a cybersecurity event. Examples of results This function falls under the following subcategories: Communications, Improvements, and Recovery Planning.

RECOVER
IDENTIFY
CYBERSECURITY FRAMEWORK
RESPOND
PROTECT
DETECT
5 YEAR ANNIVERSARY

Tools

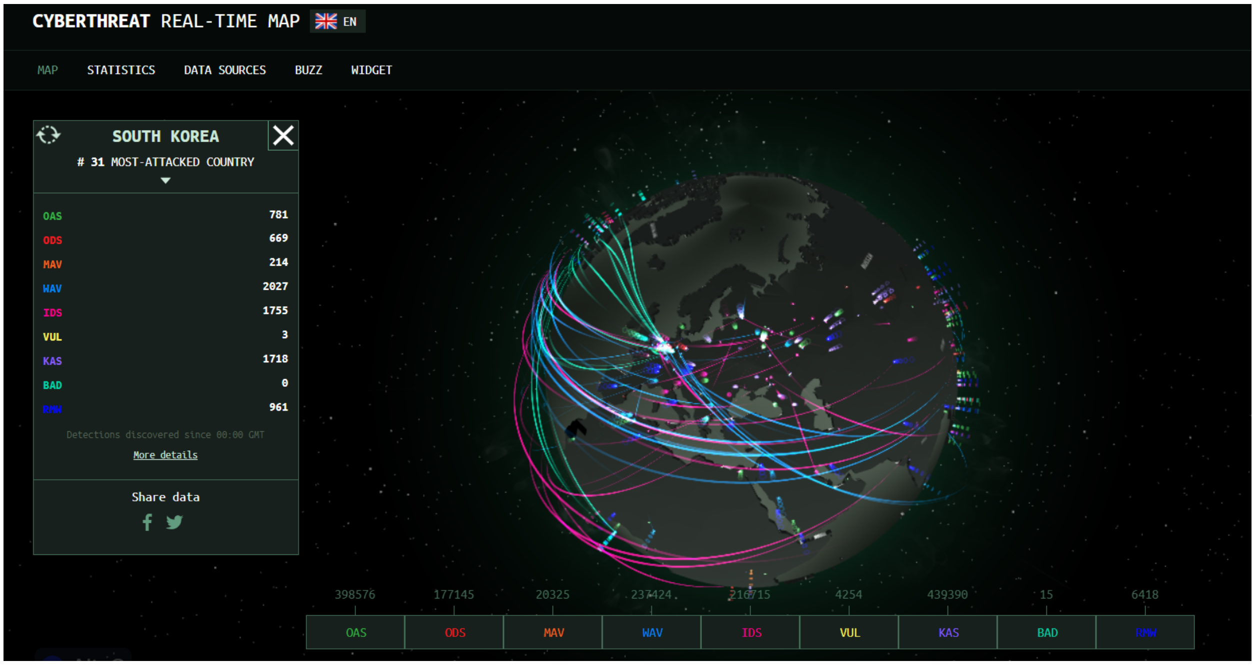
Education and awareness are two of the most vital strategies for increasing cybersecurity. Online resources are widely available and offer advice and best practices for remaining safe. These include official websites, blogs about cybersecurity, and online guides. Additionally, a lot of businesses and organizations provide their consumers and staff with cybersecurity education and awareness initiatives.

Another crucial instrument for increasing cybersecurity is antivirus software. Antivirus software provides defense against viruses, malware, and other online dangers. Numerous antivirus programs are offered, ranging from basic free versions to more sophisticated premium versions. To make sure that antivirus software is able to identify and defend against the most recent threats, it is crucial to periodically update it.

Another crucial instrument for enhancing cybersecurity is the firewall. Firewalls aid in limiting illegal access to a network or computer. They might be hardware- or software-based, and they're usually set up to stop incoming traffic from unreliable sources.

The use of password managers is yet another technology that can support cybersecurity. It is simpler to set strong, individual passwords for each account when using password managers, which securely store login information for several websites and applications. In the case that one password is hacked, this can assist in preventing hackers from getting access to several accounts.

Finally, virtual private networks (VPNs) are a tool that, by encrypting internet traffic and disguising the user's IP address, can support cybersecurity. VPNs are frequently used by remote employees to securely access company networks, but they can also be used by regular citizens to shield themselves from government and hacker eavesdropping and spying.



SOUTH KOREA

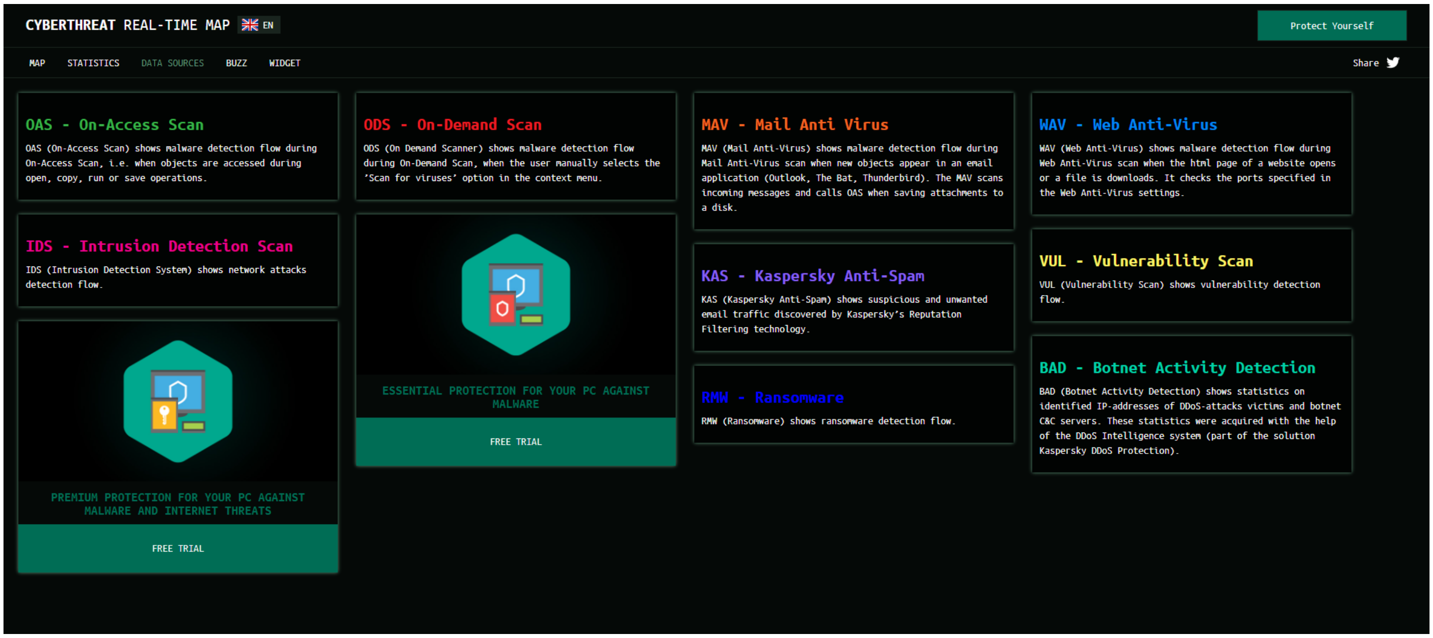
31 MOST-ATTACKED COUNTRY

OAS	781
ODS	669
MAV	214
WAV	2027
IDS	1755
VUL	3
KAS	1718
BAD	0
RMW	961

Detections discovered since 00:00 GMT

398576	177145	20325	237424	216715	4254	439390	15	6418
OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD	RMW

The illustration above also shows how certain third parties have public tools that allow us to gather data on recent cyber attacks. The Kaspersky cyber attack graph (that is update in real time) shows how civilians are able to protect themselves against cyber criminals and state actors.


CYBERTHREAT REAL-TIME MAP
EN
Protect Yourself
MAP
STATISTICS
DATA SOURCES
BUZZ
WIDGET
Share
PREMIUM PROTECTION FOR YOUR PC AGAINST MALWARE AND INTERNET THREATS
FREE TRIAL
ESSENTIAL PROTECTION FOR YOUR PC AGAINST MALWARE
FREE TRIAL

OAS - On-Access Scan

OAS (On-Access Scan) shows malware detection flow during On-Access Scan, i.e. when objects are accessed during open, copy, run or save operations.

IDS - Intrusion Detection Scan

IDS (Intrusion Detection System) shows network attacks detection flow.

ODS - On-Demand Scan

ODS (On Demand Scanner) shows malware detection flow during On-Demand Scan, when the user manually selects the 'Scan for viruses' option in the context menu.

MAV - Mail Anti Virus

MAV (Mail Anti-Virus) shows malware detection flow during Mail Anti-Virus scan when new objects appear in an email application (Outlook, The Bat, Thunderbird). The MAV scans incoming messages and calls OAS when saving attachments to a disk.

KAS - Kaspersky Anti-Spam

KAS (Kaspersky Anti-Spam) shows suspicious and unwanted email traffic discovered by Kaspersky's Reputation Filtering technology.

RMW - Ransomware

RMW (Ransomware) shows ransomware detection flow.

WAV - Web Anti-Virus

WAV (Web Anti-Virus) shows malware detection flow during Web Anti-Virus scan when the html page of a website opens or a file is downloads. It checks the ports specified in the Web Anti-Virus settings.

VUL - Vulnerability Scan

VUL (Vulnerability Scan) shows vulnerability detection flow.

BAD - Botnet Activity Detection

BAD (Botnet Activity Detection) shows statistics on identified IP-addresses of DDoS-attacks victims and botnet C&C servers. These statistics were acquired with the help of the DDoS Intelligence system (part of the solution Kaspersky DDoS Protection).

Conclusions

In conclusion, the US government is committed to ensuring the online safety of its citizens from foreign cyber threats through various initiatives and collaborations. Citizens also play a crucial role in protecting themselves from foreign attackers by taking steps such as using strong passwords, enabling two-factor authentication, and remaining vigilant against phishing scams. Together, these efforts can help safeguard the digital ecosystem and protect the privacy and security of all citizens. With the emerging technology of VPNs and organizations such as Kaspersky and NIST allow people to be protected from malicious activity online. In the end, it is a community effort to keep people aware of the malicious cyber activity around and that is why open forums like Kapersky are so valuable because it allows normal citizens to have some cyber threat intelligence without the help of the government.

Works Cited

National Security Agency/Central Security Service > Culture > Operating Authorities. (n.d.). Www.nsa.gov.

https://www.nsa.gov/Culture/Operating-Authorities/#:~:text=One%20of%20NSA%27s%20core%20values%20is%20respect%20for

Homeland Security. (2022, September 26). Cybersecurity | Homeland Security. Www.dhs.gov. https://www.dhs.gov/topics/cybersecurity

Zahid, I. (2022, February 4). Cyber Diplomacy: An Emerging Strategy of Foreign Policy - Cyber Insights. https://www.cyber-insights.org/cyber-diplomacy-an-emerging-strategy-of-foreign-policy/

What is a VPN? (n.d.). Us.norton.com. https://us.norton.com/blog/privacy/what-is-a-vpn

Is private browsing and VPN really secure? (2020, July 9). Usa.kaspersky.com. https://usa.kaspersky.com/resource-center/definitions/how-does-vpn-keep-me-safe-online

Cyber Issues. (2020, January 22). US Department of State. https://www.state.gov/policy-issues/cyber-issues/

NIST. (2019, July 8). Cybersecurity Framework. NIST. https://www.nist.gov/cyberframework

About CISA | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/about

Nist Risk Management Framework. (n.d.). Nist Risk Management Framework. https://damienyouthgonzalez.blogspot.com/2022/09/nist-risk-management-framework.html