Virginia Department of Emergency Management

www.vaemergency.gov
facebook.com/VAemergency
@VDEM

CYBERSECURITY IN VIRGINIA

National Cybersecurity Awareness Month (NCSAM) held each October is intended to ensure every American has the resources they need to stay safe online. Cybersecurity is a 24/7, 365 days a year, concern and threat. Virginians need to consistently prepare for and be vigilant of evolving cybersecurity threats. Cybersecurity is not just the responsibility of government, companies, groups or individuals. Everyone shares the responsibility for cybersecurity - from the average smartphone user to the corporate CEO.

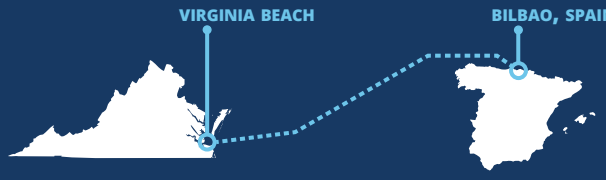
There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Virginia is home to all 16 sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors; transportation systems; and water and wastewater systems. Virginians and businesses located in the Commonwealth should use NCSAM to re-acquaint themselves with best practices for online safety and privacy to protect their homes and workplaces.

CRITICAL INFRASTRUCTURE IN THE COMMONWEALTH

Northern Virginia is home to **4 of the top 10 cloud campuses** in the U.S. No other market has more than one.

On any given day, **70 percent of the world's internet traffic** passes through data centers located in Loudoun County—roughly **2.2 million terabytes of data**. Loudoun has the largest concentration of data centers in the world.

Facebook chose Henrico County to construct its 11th data center, a nearly **$2 billion investment, totaling 1.5 million square feet**.



A **4,000 mile-long transatlantic cable**, named Marea, (Spanish for "tide") links Virginia Beach and Bilbao, Spain. The cable can transmit **160 terabits** of data per second, making it the highest capacity data cable crossing the Atlantic Ocean. This cable gives companies access to another **1 billion internet users**.

CYBERSECURITY AT HOME

MAINTAIN YOUR DEVICES

» Keep all software on internet-connected devices current to reduce the risk of infection from ransomware and malware. Regularly scan your devices for viruses and spyware. Visit www.stopthinkconnect.org for more ways to protect your devices.

STRENGTHEN YOUR PASSWORD

» Avoid using common words, phrases or well-known information about yourself in your passwords. Instead, create a password with eight characters or more with a combination of letters, numbers and symbols. Additionally, always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email, medical files or bank accounts. For more tips and tricks to protect your password, visit www.dhs.gov.

BACK IT UP

» Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup source.

CONNECT SAFELY

» Before you connect to any public wireless hotspot – like on an airplane or in an airport or hotel – be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. For more useful tips about secure Wi-Fi visit www.dhs.gov.

SET PRIVACY SETTINGS

» Use privacy and security settings on social media platforms and other sites to control who has access to your public and personal information. It's OK to limit how and with whom you share information.

SHARE RESPONSIBLY

» Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others. Maintain an open dialogue with your friends, family, colleagues, community and especially children about internet safety.

CYBERSECURITY FOR SMALL BUSINESSES

ADDRESS YOUR RISK

» Use the Department of Homeland Security's C³ Voluntary Program Small and Midsize Business Toolkit for resources to help your business recognize and address cybersecurity risks.

MAKE A PLAN

» Create a custom cybersecurity plan for your small business with the Federal Communication Commission's (FCC) Small Biz Cyber Planner 2.0. Visit www.FCC.gov for more tips on how to protect your small business from potential cyber threats.

SECURE YOUR NETWORK

» Get information from the United States Computer Emergency Readiness Team (US-CERT) on how to secure your business network and protect your company from security breaches.

PROTECT YOURSELF AND OTHERS

» Safeguard your business, employees, and customers from online attacks, data loss, and other threats with resources from the National Cyber Security Alliance. Learn about compliance resources on collecting sensitive data from consumers and employees from the Federal Trade Commission.

DATA BREACHES

Protection from data breaches and identity theft have become a part of our everyday lives. Large scale data breaches have occurred with some of our nation's biggest retailers, like Target and Home Depot, but they have also occurred through federal agencies, like the Office of Personnel Management.

The Department of Homeland Security and National Cyber Security Alliance provide invaluable tools to increase our cybersecurity awareness. The Department of Homeland Security's 'Stop.Think.Connect.' campaign is a national public awareness effort aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Visit www.dhs.gov for more information on how to get involved with the 'Stop.Think. Connect.' campaign.

CYBER-INCIDENT REPORTING

A cyber incident is an event that could jeopardize the confidentiality, integrity or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the federal government. Victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions;
- or impact national security, economic security, or public health and safety.

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector-specific agency, and any of the federal agencies listed here. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, they should comply and voluntarily report the incident to an appropriate federal point of contact.

TRAINING

- Federal Virtual Training Environment is a free online cybersecurity training system that is available at no charge for government personnel and Veterans. It contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.