CyberAware

Awareness Through Information Sharing

Incidents/Articles of Note:

- School District's Files Leaked in $40m Ransomware Attack
- Houston Rockets Hit by the "Babuk" Ransomware Gang
- 1-Click Hack Found in Popular Desktop Apps — Check If You're Using Them
- Over 750,000 Users Downloaded New Billing Fraud Apps From Google Play Store
- Apple AirDrop Bug Could Leak Your Personal Info to Anyone Nearby
- Update Your Chrome Browser ASAP to Patch a Week Old Public Exploit
- Malware Variants: More Sophisticated, Prevalent and Evolving in 2021
- Cyber-attack on NBA Team
- 80% of Global Enterprises Report Firmware Cyberattacks
- How Email Attacks are Evolving in 2021

Resource - DHS CISA

Stop. Think. Connect. Toolkit

Cyber criminals do not discriminate; they target vulnerable computer systems regardless of whether they are part of a large corporation, a small business, or belong to a home user. Cybersecurity is a shared responsibility in which all Americans have a role to play. The STOP. THINK. CONNECT. ™ Toolkit provides resources for all segments of the community.

View Resource

Resource - DHS CISA

Emergency Operations Plans for Houses of Worship

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

View Resource

DHS and NASCIO

Cybersecurity Governance in the Commonwealth of Virginia

This case study describes how the Commonwealth of Virginia (the Commonwealth) has used laws, policies, structures, and processes to help govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders.

View Case Study

Resource - FBI

The Cyber Threat

Malicious cyber activity threatens the public's safety and our national and economic security. The FBI's cyber strategy is to impose risk and consequences on cyber adversaries. Our goal is to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves.

View Resource

This is an open-source product. Redistribution is encouraged.

View Virginia Fusion Center Homepage

Click Here

Observe Suspicious Activity?

Report Online

"Awareness Through Information Sharing"

This product is the result of collaboration and cooperation with the following Shield partners.

Need Help with this Email?

View in a browser

Download as a PDF

Useful Links

- VFC Fusion Site
- Shield Homepage
- All Products
- Report SAR
- Email Coordinator

VFC Shield

"Awareness Through Information Sharing"
