CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

COMMUNITY BULLETIN

Announcements

CISA Launches Public Awareness Initiative Urging Cybersecurity Around Holiday Shopping Season

As the busiest shopping season of the year, the holidays frequently see an uptick in cybercrime and scams. To inform the public of common cybersecurity risks, the Cybersecurity and Infrastructure Security Agency (CISA) has launched a website complete with easy-to-follow safety tips for online shopping and a video message from CISA Director Christopher Krebs.

“The holiday season is a prime time for hackers, scammers, and online thieves,” said Director Krebs. “The good news is you don’t need to be a cybersecurity pro to defend yourself. It’s often the simple things that make a big difference in protecting yourself and your family from cyber threats and scams. We’re sharing these simple steps to keep consumers safe while shopping online for the best deals and gifts this holiday season.”

While the site includes several security and safety tips, CISA recommends starting with these three simple steps to keep consumers safe when shopping online:

- **Check your devices** – Before starting the hunt for the best deal, make sure your devices are up-to-date and your accounts have strong passwords. Once you’ve purchased an internet-connected device or toy, change the default password and check the device’s privacy and security settings to ensure you’re not sharing more information than you want.
- **Shop through trusted retailers** – Before making a purchase and providing any personal or financial information, make sure you’re using a reputable, established vendor.
- **Using safe methods for purchases** – If you can, use a credit card as opposed to a debit card since credit cards often have better fraud protections.

For more information about shopping online safely this holiday season, visit www.CISA.gov/shop-safely.

CISA Invests in Cutting-Edge Election Security Auditing Tool Ahead of 2020 Elections

CISA is teaming up with election officials and their private sector partners to develop and pilot an open source post-election auditing tool ahead of the 2020 elections. The tool is being created by VotingWorks, a non-partisan, non-profit organization dedicated to building secure election technology. CISA’s investment is designed to support election officials and their private sector partners who are working to improve post-election auditing in the 2020 election and beyond. The tool supports numerous types of post-election audits across various types of voting systems, including all major vendors.

“Heading into 2020, we’re exploring all possible ways that we can support state and local election officials while also ensuring Americans across the country can confidently cast their votes,” said CISA Director Christopher Krebs. “At a time when we know foreign actors are attempting to interfere and cast doubt on our democratic processes, it’s incredibly important elections are secure, resilient, and transparent. For years, we have promoted the value of auditability in election security; it was a natural extension to support this open source auditing tool for use by election officials and vendors, alike.”

Learn more about the auditing tool in the press release on the CISA website.

Events

Partner Webcast: You Don't Say: An FTC Workshop on Voice Cloning Technologies

On January 28, 2020, the Federal Trade Commission (FTC) will examine voice cloning technologies that enable users to make near-perfect reproductions of a real person’s voice. Advances in artificial intelligence and text-to-speech (TTS) synthesis have allowed researchers to create a near-perfect voice clone with less than a five second recording of a person’s voice.

There are a number of promising uses for this technology, such as editing the work of voice actors and enabling people with tracheotomies and other conditions to use TTS systems using voices derived from their previously-recorded audio samples. However, it also has the potential to cause substantial harm when used maliciously.

For instance, many consumers already fall prey to “grandparent scams” (where an elderly person receives a phone call supposedly from a grandchild in distress who needs cash) and phishing scams (where an employee is contacted by a superior and directed to immediately wire funds to a vendor). Voice cloning may make it harder for consumers to identify these sorts of social engineering scams.

Join the FTC as they discuss how these voice cloning technologies are developed and deployed, from healthcare and consumer-oriented applications, to fraudulent schemes.

- **Date:** Tuesday, January 28, 2020
- **Time**: 12:30 p.m. ET
- **Webcast Link**: To access the live webcast, visit FTC’s event page.

Featured Resources

Just Launched: Students Page on the National Initiative for Cybersecurity Careers and Studies Website

While many kids are home for the holidays in the coming days and weeks, now is a great time for parents to talk with them about future career opportunities, specifically in cybersecurity. With more than 300,000 cybersecurity jobs currently available across the United States, the demand for qualified professional is greater than ever.

JOB PROFILE:

CYBER FORENSICS EXPERT

Ye

+$70

+2

CISA

JOB PROFILE:

CYBER DEFENSE INCIDENT RESPONDER

DEGREE REQUIRED?

No

Bachelor's Degree in Cybersecurity or Computer Science is a plus though

MEDIAN SALARY

+$80,000

JOB GROWTH

+20%

SOFT SKILLS

Capable of Handling Stress
Flexible
Problem Solving
Analytical
Good Communication

COMMON JOB DUTIES

- Actively monitor systems and networks for intrusions
- Identify security flaws and vulnerabilities
- Perform security audits, risk analysis, network forensics and penetration testing
- Perform malware analysis and reverse engineering
- Develop a procedural set of responses to security problems
- Establish protocols for communication within an organization and dealings with law enforcement during security incidents
- Create a program development plan that includes security gap assessments, policies, procedures, playbooks, training and tabletop testing
- Produce detailed incident reports and technical briefs for management, admins and end-users
- Liaison with other cyber threat analysis entities

CISA

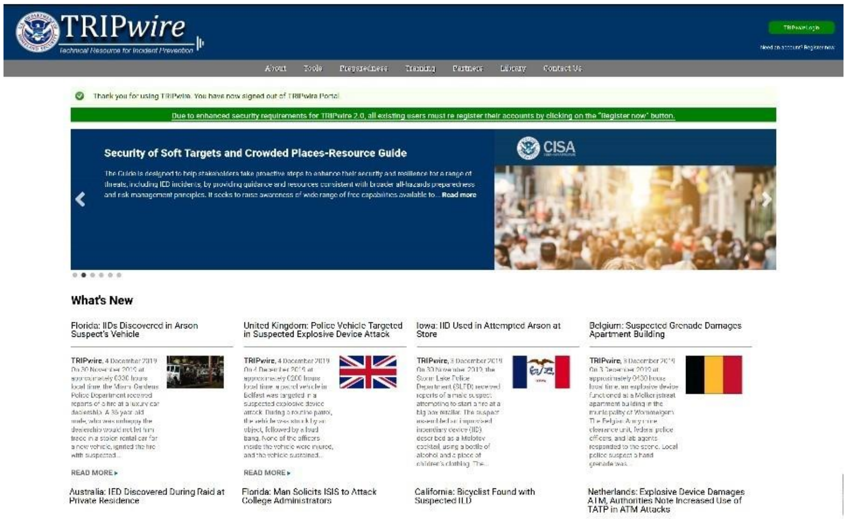
NICCS

The new Students page on the National Initiative for Cybersecurity Careers and Studies (NICCS) website provides a great introduction to the rapidly expanding field of cybersecurity. This new webpage includes 15 cybersecurity career profiles, college and scholarship information, downloadable guides, and much more to help students think about cybersecurity as a lucrative career option.

To find more information about cybersecurity concepts, academic opportunities, local events, and cybersecurity career options, explore the NICCS website and check out the Students Guide.

TRIP*wire* Website to Prepare for Improvised Explosive Device Threats

TRIPwire, the Technical Resource for Incident Prevention, is a free, online information and resource sharing portal for the nation's security and emergency services professionals. It is designed to increase their awareness of evolving improvised explosive device (IED) tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information.



Thank you for using TRIPwire. You have now signed out of TRIPwire Portal.

Due to enhanced security requirements for TRIPwire 2.0, all existing users must re-register their accounts by clicking on the "Register now" button.

Security of Soft Targets and Crowded Places-Resource Guide

The Guide is designed to help stakeholders take proactive steps to enhance their security and resilience for a range of threats, including IED incidents, by providing guidance and resources consistent with broader all-hazards preparedness and risk management principles. It seeks to raise awareness of wide range of free capabilities available to... Read more

What's New

Florida: IIDs Discovered in Arson Suspect's Vehicle

TRIPwire, 4 December 2019
On 30 November 2019 at approximately 0330 hours local time, the Miami Gardens Police Department received reports of a fire at a luxury car dealership. A 35-year-old male, who was unhappy the dealership would not let him trade in a stolen rental car for a new vehicle, ignited the fire with suspected...

READ MORE ▸

United Kingdom: Police Vehicle Targeted in Suspected Explosive Device Attack

TRIPwire, 4 December 2019
On 4 December 2019 at approximately 0200 hours local time, a patrol vehicle in Belfast was targeted in a suspected explosive device attack. During a routine patrol, the vehicle was struck by an object, followed by a loud bang. None of the officers inside the vehicle were injured, and the vehicle sustained...

READ MORE ▸

Iowa: IID Used in Attempted Arson at Store

TRIPwire, 3 December 2019
On 30 November 2019, the Storm Lake Police Department (SLPD) received reports of a male suspect attempting to start a fire at a big box retailer. The suspect assembled an improvised incendiary device (IID) described as a Molotov cocktail, using a bottle of alcohol and a piece of children's clothing. The...

Belgium: Suspected Grenade Damages Apartment Building

TRIPwire, 3 December 2019
On 3 December 2019 at approximately 0430 hours local time, an explosive device functioned at a Molkerijstraat apartment building in the municipality of Wommelgem. The Belgian Army mine clearance unit, federal police officers, and lab agents responded to the scene. Local police suspect a hand grenade was...

Australia: IED Discovered During Raid at Private Residence

Florida: Man Solicits ISIS to Attack College Administrators

California: Bicyclist Found with Suspected IED

Netherlands: Explosive Device Damages ATM, Authorities Note Increased Use of TATP in ATM Attacks

Developed and maintained by CISA's Office for Bombing Prevention, TRIP*wire* enhances domestic preparedness by giving the nation's security and emergency services professionals across the private sector and federal, state, local, tribal, and territorial entities valuable information and resources to prevent, protect against, respond to, and mitigate bombing incidents.

TRIP*wire* provides expert intelligence analysis and reports, along with awareness products, training opportunities, and videos.

Features include:

- Large volume of public-facing content,
- Coverage and analysis of the latest domestic and international IED-specific events,
- Library featuring dynamic content navigation and search,
- Access to a broad range of counter-IED training,
- Interactive domestic IED incident map and more.

This insight enables communities to identify explosive hazards and potential terrorist tactics, as well as to discover common site vulnerabilities and take advantage of other actionable information from TRIP*wire*.

To learn about evolving IED tactics, techniques, and procedures, sign up for a TRIP*wire* account at https://tripwire.dhs.gov. For assistance registering on the site, please contact the TRIP*wire* Helpdesk at 866-987-9473, or email TripWireHelp@dhs.gov.

For more information about OBP's other counter-IED resources, please visit www.cisa.gov/obp or email obp@cisa.dhs.gov.

Social Media

Help CISA spread the word about upcoming events and new resources by sharing the following posts via your social media channels. Thank you for your support!

- Did you know the holiday season is prime time for online scammers? Learn how to defend yourself by visiting the new @CISAgov site: www.cisa.gov/shop-safely #shopsafely
- Voice cloning technologies could be used maliciously. Do you know how your business might be impacted? Watch this live webcast from @FTC on Jan 28 to find out! https://www.ftc.gov/news-events/events-calendar/you-dont-say-ftc-workshop-voice-cloning-technologies
- Do you know kids interested in cybersecurity careers? The new @CISAgov Students page is a great intro to the rapidly expanding field! https://go.usa.gov/xpPAw

The CISA Community Bulletin is a monthly newsletter featuring cybersecurity and infrastructure security resources, events, and updates from CISA and its partners. Learn more at https://www.cisa.gov.

This product is provided subject to this Notification and this Privacy & Use policy.

This email was sent to egli@waterisac.org using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870

GOVDELIVERY