AUGUST
2024

CYBER ESPIONAGE

JOB AID

CONTENTS

INTRODUCTION

WHAT IS CYBER ESPIONAGE?

The malicious theft of data, information, or intellectual property from, and/or through computer systems. Unlike traditional espionage, which might involve physical infiltration or human intelligence sources (HUMINT), cyber espionage leverages malware, spyware, and phishing attacks to exploit vulnerabilities in computer systems and networks. Some methods include social engineering, malware distribution, advanced persistent threat (APT), watering hole attacks, and spear phishing, but this list is by no means all-inclusive.

WHAT MAKES CYBER ESPIONAGE DIFFERENT?

One significant aspect of cyber espionage is its global reach and anonymity. Cyber-attackers can conduct their activities across continents without ever leaving their desks. This ability not only makes it challenging for victims to detect and respond effectively, but also complicates international legal responses due to jurisdictional limitations and varying laws on cybercrime.

WHY IS AN UNDERSTANDING OF CYBER ESPIONAGE SO IMPORTANT?

The complexity of these operations varies greatly. Some are meticulously planned campaigns targeting specific entities over extended periods—often employing APTs that dwell undetected within networks—while others may be more opportunistic in nature. The motives behind such acts also span a broad spectrum from state-sponsored efforts to gain geopolitical leverage, to corporate espionage where competitive secrets are the prize.

FOR WHOM WAS THIS JOB AID CREATED?

This job aid is designed to give individuals a better understanding of cyber espionage. This job aid will provide individuals with a baseline understanding and provide information that can be used to become better versed in the threat actors, tactics, tools, and procedures used to compromise your systems and devices.

HOW SHOULD THIS JOB AID BE USED?

This job aid is not all-inclusive. Use it as a tool to develop additional understanding of cyber espionage and for guidance on how organizations can protect their missions and priorities. Use it as a reminder of the exceptional duty of care vested in those with access to information and critical infrastructure systems.

CYBER ESPIONAGE VS. CYBER WARFARE

Espionage is the activity of gathering secret or sensitive information for personal gain, technological purposes, or politics. Cyber warfare, on the other hand, involves attacking and damaging critical computer systems and infrastructure. The intent is not just to steal information but to destabilize, disrupt, and deny access to critical systems.

Cyber espionage is a precursor to cyber warfare. Cyber warfare is becoming more prevalent as global conflicts between nations continue, with Ukraine acting as a testbed for tactics, tools, and procedures.

EXAMPLES OF CYBER WARFARE

OCTOBER 10, 2022 - SANDWORM/CADDYWIPER

Russian threat actors carried out a multi-day attack disrupting Ukrainian power distribution. The threat actors deployed malware in the target's environment to cause further disruption and potentially remove forensic artifacts that could lead to the discovery of the operation.

2022 Ukraine Electric Power Attack, Campaign C0034 | MITRE ATT&CK®

JULY 22, 2022 - HOMELAND JUSTICE

Iranian state cyber actors launched a destructive cyber-attack against the government of Albania which rendered websites and services unavailable.

Iranian State Actors Conduct Cyber Operations Against the Government of Albania | CISA

JANUARY 15, 2022 - WHISPERGATE

Threat actors deployed destructive malware against organizations in Ukraine to destroy computer systems and render them inoperable.

Update: Destructive Malware Targeting Organizations in Ukraine | CISA

DECEMBER 2016 - SANDWORM/INDUSTROYER

Russian cyber actors used Industroyer malware to target and disrupt substations within Ukraine causing power outages.

Office of Public Affairs | Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace | United States Department of Justice

DECEMBER 23, 2015 - SANDWORM/BLACKENERGY

Ukrainian power companies experienced unscheduled power outages impacting many customers in Ukraine.
Cyberattack Against Ukrainian Critical Infrastructure | CISA

LEARN MORE

When it concerns national security, proper training and protections must be applied to our Nation's critical infrastructure. CDSE offers many industrial training programs and materials. The Industrial Security Basics course is a great place to start:

Industrial Security Basics IS122.16 (cdse.edu)

MOTIVATIONS OF CYBER ESPIONAGE

There are a multitude of motives that drive individuals and entities to engage in cyber espionage. Understanding these motivations is crucial for developing effective defenses and policies.

FINANCIAL GAIN

The prospect of financial rewards is a strong motivator. Examples include direct theft from bank accounts, selling stolen passwords, or deploying ransomware to extort money from victims.

RECOGNITION

Small groups and some individual hackers thrive on the challenge and notoriety of breaching highly secure systems.

INSIDER THREATS

Some threats come from trusted insiders. Personnel with access might exploit their position due to grievances against their employer, financial incentives, or even coercion by external parties.

POLITICAL

Political ideologies can be motivation to hack persons or organizations as a form of activism or hacktivism.

CORPORATE ESPIONAGE

Businesses may engage in spying activities against competitors to gain critical insights into proprietary processes, upcoming products, and marketing strategies.

STATE-SPONSORED

Governments deploy cyber espionage tactics for military advantage, economic advantages, and political leverage. State cyber operations aim to collect diplomatic intelligence, find weaknesses in infrastructures, influence foreign policy decisions, and gain advanced technological materials without investing time and resources in Research and Development.

Motivations can be for personal gain or can involve state-endorsed organizations attempting to obtain all the above. It's crucial for governments, corporations, and individuals to adopt a holistic approach that combines robust technological defenses, dedicated training, and information sharing.

LEARN MORE

An individual's office, position, or security clearance alone may not reduce the likelihood of being the target of cyber espionage. It is recommended that personnel regularly attend training for better situational awareness. The CDSE offers a Counterintelligence Awareness and Security Brief training:

Counterintelligence Awareness and Security Brief CI112.16 (cdse.edu)

TARGETS OF CYBER ESPIONAGE

Cyber espionage casts a wide net over potential targets, each chosen for the unique and valuable data they hold.

BUSINESSES

Large corporations to small businesses.

- **Internal Information**

  Examples include company structure, operational data, research and development data, and salaries.

- **Information on clients and customers**

  Examples include a list of clients, what services are provided, cost, as well as marketing and services.

- **Market and competitors**

  Examples include data regarding the marketing goals of an organization and knowledge about its competitors with the purpose of exploiting unfair market conditions.

RESEARCH

Particularly in STEM (science, technology, engineering, and mathematics), dual-use technologies, emerging technology, and other commercially sensitive areas could be of interest to other states.

INFORMATION/PROPERTY

Examples include data related to proprietary formulas, secret projects, internal plans, or information related to projects and development.

GOVERNMENT AGENCIES

Examples include information related to national security and policymaking, including military secrets, diplomatic communications, and internal strategies.

POLITICAL INFORMATION

Examples include confidential government information, negotiating positions, sensitive economic information, and details of policy developments.

MILITARY INFORMATION

Examples include information on weapon systems, troop locations, and information on defenses.

ACTIVITIES OF DISSIDENTS

Foreign governments may choose to target dissident movements and individuals in the U.S. that they see as a threat to their control at home. These activities can be aimed to gather information, create insider threats, or collect targets for intimidation.

LEARN MORE

Foreign adversaries seek to exploit vulnerabilities within DOD institutions through infiltration, coercion, or recruitment of personnel. Additional resources can be found on the Foreign Considerations Job Aid: potential_risk_indicators_foreign_considerations.pdf (cdse.edu)

CYBER ESPIONAGE EXAMPLES

- **The three Chinese hackers work for the purportedly China-based internet security firm Guangzhou Bo Yu Information Technology Company Limited (a/k/a "Boyusec").**

  In November 2017, Wu Yingzhuo, Dong Hao, and Xia Lei, Chinese nationals and residents of China, were charged with computer hacking, theft of trade secrets, conspiracy, and identity theft. Between 2011 and May 2017, these efforts were directed at U.S. and foreign employees, and three corporations in the financial, engineering, and technology industries.

  Office of Public Affairs | U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage | United States Department of Justice

- **U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts**

  In March 2017, the United States Department of Justice indicted two FSB officials and their Russian cybercriminal conspirators on computer hacking and conspiracy charges related to the collection of emails of U.S. and European employees of transportation and financial service firms. The charges included conspiring to engage in economic espionage and theft of trade secrets.

  Office of Public Affairs | U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts | United States Department of Justice

- **Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps**

  In March 2018, nine Iranian hackers associated with the Mabna Institute were charged with stealing intellectual property from more than 144 U.S. universities which spent approximately $3.4 billion to procure and access the data. The data was stolen at the behest of Iran's Islamic Revolutionary Guard Corps and used to benefit the government of Iran and other Iranian customers, including Iranian universities. Mabna Institute actors also targeted and compromised 36 U.S. businesses.

  Office of Public Affairs | Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps | United States Department of Justice

LEARN MORE

Cyber economic espionage is one facet of the much larger global economic espionage challenge. The National Counterintelligence and Security Center (NCSC) compiled this report for additional information: 20180724-economic-espionage-pub.pdf (dni.gov)

NATION-STATE CYBER ACTORS

Nation-State actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information.

Nation-state adversaries pose an elevated threat to our national security. These adversaries are known for their advanced persistent threat (APT) activity. APT actors are well-resourced and engage in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion. APT objectives could include espionage, data theft, and network/system disruption or destruction.

APTs:

The People's Republic of China (PRC)

Engages in malicious cyber activities to support its strategic development goals of science and technology advancement, military modernization, and economic policy objectives, including **infiltrating critical infrastructure networks**.

The Russian Federation

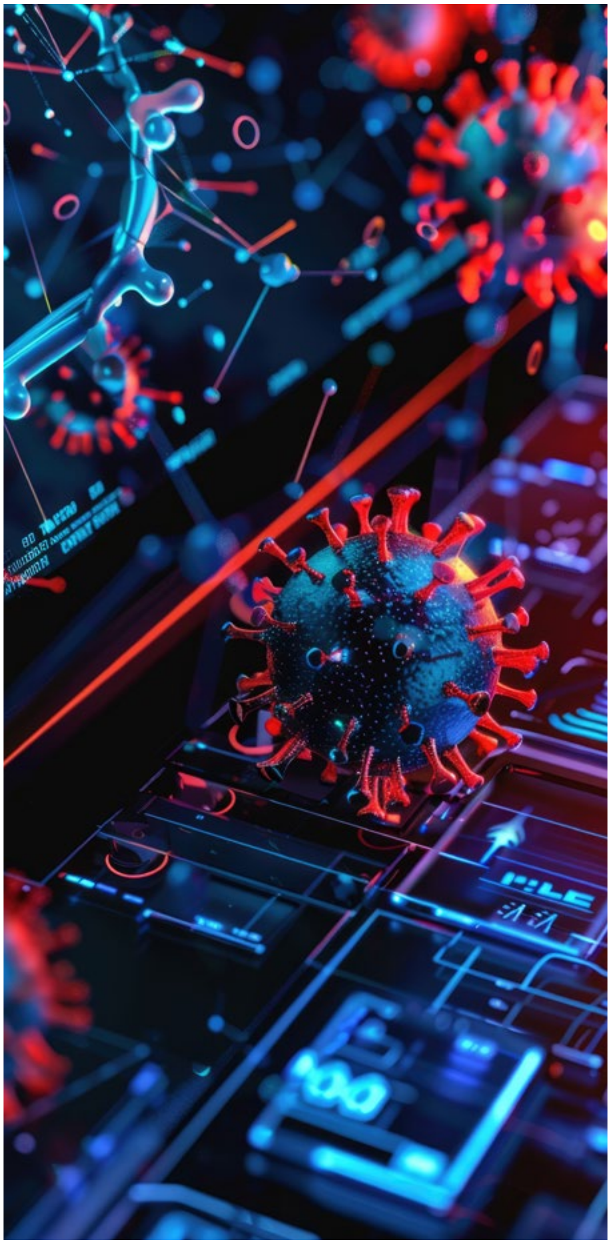
Engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress both international and internal social and political activity, to steal intellectual property, and to harm regional and international adversaries.

The Democratic People's Republic of Korea (DPRK)

Employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.

The Islamic Republic of Iran

Has exercised its increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries.



LEARN MORE

Nation-state adversaries pose an elevated threat to our national security. These adversaries are known for their advanced persistent threat (APT) activity. CISA provides additional resources and information on the roles and threat of the largest threats to U.S. cyber security.

Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA.

METHODS USED BY FOREIGN INTELLIGENCE SERVICES

State threats exist online and offline. While a wide range of hostile actors use the internet to target people in the U.S., state actors are well equipped to conduct the most damaging online operations. States and other hostile actors may look to steal information remotely. Stealing information remotely enables them to do so on an industrial scale with relatively little risk to their intelligence officers or overseas agents and at little cost. They may also use malicious software, also known as malware, to disrupt and damage infrastructure. This can range from taking a website offline to manipulating industrial systems.

ELICITATION

An effort in which a seemingly normal conversation is contrived to extract information about individuals, their work, and their colleagues.

EAVESDROPPING

Gathering information in social environments by listening in on private conversations.

BAG OPERATIONS

Efforts to steal, photograph, or photocopy documents, magnetic media, and laptop computers. This could occur in your hotel room, in an airport, in a conference room, or in any other situation where the opportunity presents itself and your materials are vulnerable.

ELECTRONIC INTERCEPTION

Use of devices to electronically monitor an individual's use of modern telecommunications, office, hotel, portable telephones, faxes, and computers.

TECHNICAL EAVESDROPPING

Use of audio and visual devices, usually concealed in hotel rooms, restaurants, offices, cars, and airplanes.

LEARN MORE

Foreign intelligence services may use an individual's (insider's) digital footprint data to understand their pattern of life, preferences, and susceptibilities. CDSE's Insiders Digital Footprint Job Aid can help identify and reduce your digital footprint:

insiders-digital-footprint.pdf (cdse.edu)

WHAT IS A CYBER ATTACK?

A cyberattack is an attempt by threat actors, hackers, or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying, or exposing information.

Cyberattacks can target a wide range of victims from individual users to enterprises, or even governments. When targeting businesses or other organizations, the hacker's goal is usually to access sensitive and valuable company resources, such as intellectual properties (IP), customer data, or financial details.

EXAMPLES:

MALWARE OR MALICIOUS SOFTWARE

Any program or code created with the intent to do harm to a computer, network, or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, crypto-jacking, and any other type of malware attack that leverages software in a malicious way.

SPYWARE

A type of unwanted, malicious software that infects a computer or other device and collects information about a user's web activity without their knowledge or consent.

WORM

A self-contained program that replicates itself and spreads its copies to other computers. A worm may infect its target through a software vulnerability, or it may be delivered via phishing or smishing. Embedded worms can modify and delete files, inject more malicious software, or replicate in place until the targeted system runs out of resources.

MOBILE MALWARE

Any type of malware designed to target mobile devices. Mobile malware is delivered through malicious downloads, operating system vulnerabilities, phishing, smishing, and the use of unsecured Wi-Fi.

LEARN MORE

Malware, phishing, and ransomware are becoming increasingly common forms of attack and can affect individuals and large organizations. The Cybersecurity and Infrastructure Security Agency (CISA) offers additional resources:

Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency CISA

WHAT IS A CYBERATTACK? *(CONTINUED)*

EXAMPLES:

PHISHING

A type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.

- **Spearphishing**
  A type of phishing attack that typically uses malicious emails to target specific individuals or organizations. The goal of spearphishing is to steal sensitive information such as login credentials or infect the targets' device with malware.

- **Smishing**
  The act of sending fraudulent text messages designed to trick individuals into sharing sensitive data such as passwords, usernames, and credit card numbers. A smishing attack may involve threat actors pretending to be your bank or a shipping service you use.

SPOOFING

A technique where a threat actor disguises themselves as a known or trusted source. In doing so, the threat actor engages with the target and access their systems or devices with the goal of stealing information, extorting money, or installing malware or other harmful software on the device.

- **Email Spoofing**
  A type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.

SOCIAL ENGINEERING

A technique where attackers use psychological tactics to manipulate people into taking a desired action. Threat actors will use motivators like heightened emotions, money, and status. Threat actors gather sensitive information to either extort an organization or leverage such information for a competitive advantage.

IDENTITY-DRIVEN

Identity-driven attacks are extremely hard to detect. When a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often very difficult to differentiate between the user's typical behavior and that of the hacker using traditional security measures and tools.

SUPPLY CHAIN ATTACK

A type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. **Software supply chain attacks** inject malicious code into an application to infect all users of an app, while **hardware supply chain attacks** compromise physical components for the same purpose. Software supply chains are particularly vulnerable because modern software is not written from scratch; rather, it involves many off-the-shelf components, such as third-party APIs, open-source code, and proprietary code from software vendors.

LEARN MORE

Cyber-attacks come in all shapes and sizes, and all levels of an organization can be targeted. This interactive training provides an explanation of various types of social engineering, including phishing, spear-phishing, whaling, smishing, and vishing. The CDSE eLearning course, Phishing and Social Engineering, offers historical examples and insight:

Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency CISA

IMPROVE YOUR RESILIENCE AGAINST CYBER THREATS

Implementing safe cybersecurity best practices is important for individuals as well as organizations of all sizes. Using strong passwords, updating your software, thinking before you click on suspicious links, and turning on multi-factor authentication are the basics of what we call "cyber hygiene" and will drastically improve your online safety.

ASSESS YOUR CURRENT STATE

Coordinate with your organization's Chief Information Security Officer (CISO) and security teams to assess your organization's current security posture and implement necessary policies, tools, and procedures to protect your systems.

CHECK ACCESS TO DATA POLICY

Monitor access to sensitive, critical information. Review the organization's policy and determining who needs access to what is the first step in protecting sensitive data.

MITIGATE RISK

Prioritize mitigation of known exploited vulnerabilities. Fix common network misconfigurations. Prioritize logging and close and/or monitor high-risk ports. Establish the principle of Zero Trust.

MONITOR UNEXPECTED BEHAVIOR

Be aware of the risk of insider threats. Configure firewalls and alerts to recognize normal behavior within the organization and to generate alerts for unexpected or abnormal behavior.

PROTECT CRITICAL INFRASTRUCTURE

Only allow users to access the network and information they need. Additionally, create policies to provide users with the necessary permissions.

REPORT MALICIOUS ACTIVITY

Report incidents as defined by NIST Special Publication 800-61 Rev 2, to include:

- Attempts to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Abuse or misuse of a system or data in violation of policy

Federal incident notification guidelines, including definitions and reporting timeframes, can be found here.

LEARN MORE

Cyberspace is particularly difficult to secure due to several factors. CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks: Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA

RECRUITMENT CYCLE USED BY FOREIGN INTELLIGENCE SERVICES

Collected intelligence information and data enables foreign intelligence officers to spot and assess individuals (insiders) for potential recruitment. Adversaries are not necessarily looking for someone with a high level of access; sometimes the potential for future access or the ability of the recruit to lead to other high value targets is enough to generate adversary interest. An insider could be targeted through unsolicited emails or social networking platforms by foreign intelligence services. Foreign intelligence officers or their co-opted organization insiders, or agents and non-traditional collectors, can target insiders to collect sensitive or classified information.

EXAMPLES:

SPOTTING

Stage of identifying potential intelligence targets.

ASSESSMENT

Learning as much as possible about the targeted individual.

RECRUITMENT

Choosing a method to recruit the individual for information, usually using a motivator of some kind such as money, ideology, compromise, or ego.

HANDLING

Recruited target begins to provide the intelligence service with classified/sensitive information.

TERMINATION

When espionage activities come to an end.

LEARN MORE

Foreign intelligence services may use an individual’s (insider’s) digital footprint data to understand their pattern of life, preferences, and susceptibilities. This CDSE Job Aid offers additional information and insight: [Foreign Intelligence Entity Targeting Recruitment Methodology Job Aid (cdse.edu)](https://cdse.edu)

REPORTING

The Federal Government conducts two main activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to the broader community. To submit a report, please select the appropriate organization for your needs:

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA):

- Incident Reporting Form
- Share Indicators and Defensive Measures
- Report Malware
- Report Software Vulnerabilities or ICS Vulnerabilities
- Report Vulnerabilities in U.S. Government Websites
- Call – 1-844-729-2472

DEPARTMENT OF HOMELAND SECURITY (DHS):

- National Cybersecurity and Communications Integration Center (NCCIC): NCCIC@hq.dhs.gov
- Call - 888-282-0870
- United States Computer Emergency Readiness Team: http://www.us-cert.gov/
- Homeland Security Investigations 1-877-4-HSI-TIP

FEDERAL BUREAU OF INVESTIGATION (FBI) - INTERNET CRIME COMPLAINT CENTER (IC3)

- Business Email Compromise
- Ransomware
- Elder Fraud
- Other Cyber Crimes
- FBI Field Office Cyber Task Forces
- National Cyber Investigative Joint Task Force: cwatch@ic.fbi.gov

UNITED STATES SECRET SERVICE:

- Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs)

DEPARTMENT OF DEFENSE (DOD):

- Department of Defense Cyber Crime Center (DC3)
    - Malware
    - Cyber Crime Center
    - DC3 Call – 410-981-0104 or 877-838-2174
- Defense Industrial Base (DIB)
    - Cybersecurity Program
    - DIB Call – 703-604-3167 or 855-363-4227

ADDITIONAL RESOURCES

APPLIED RESEARCH ON SOCIAL MEDIA AND SECURITY (WEBINAR):

Applied Research On Social Media And Security (cdse.edu)

CYBER INSIDER THREAT (eLEARNING COURSE):

Cyber Insider Threat INT280.16 (cdse.edu)

CYBERSECURITY ATTACKS - THE INSIDER THREAT (SHORT):

Cybersecurity Attacks: The Insider Threat (usalearning.gov)

CYBERSECURITY AWARENESS (ELEARNING COURSE):

https://www.cdse.edu/Training/eLearning/CS130/

POTENTIAL RISK INDICATORS: INSIDER THREAT (JOB AID):

INTJ0181-insider-threat-indicators-job-aid.pdf (menlosecurity.com)

FACEBOOK SMARTCARD:

Facebook Smart Card (cdse.edu)

LINKEDIN SMARTCARD:

LinkedIn Smartcard Trifold (cdse.edu)

TWITTER SMARTCARD:

Twitter Smart Card (cdse.edu)

YOUR EVOLVING DIGITAL LIFE (WEBINAR):

Your Evolving Digital Life (cdse.edu)

PROTECT YOURSELF FROM TRACKING TECHNOLOGIES AND SPYWARE:

https://www.cisa.gov/resources-tools/training/follow-cybersecurity-best-practices-protect-yourself-tracking-technologies-and-spyware

PROTECT THE DATA THAT IS STORED ON YOUR DEVICES:

https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices