An Insider's Digital Footprint and Associated Risks

JOB AID

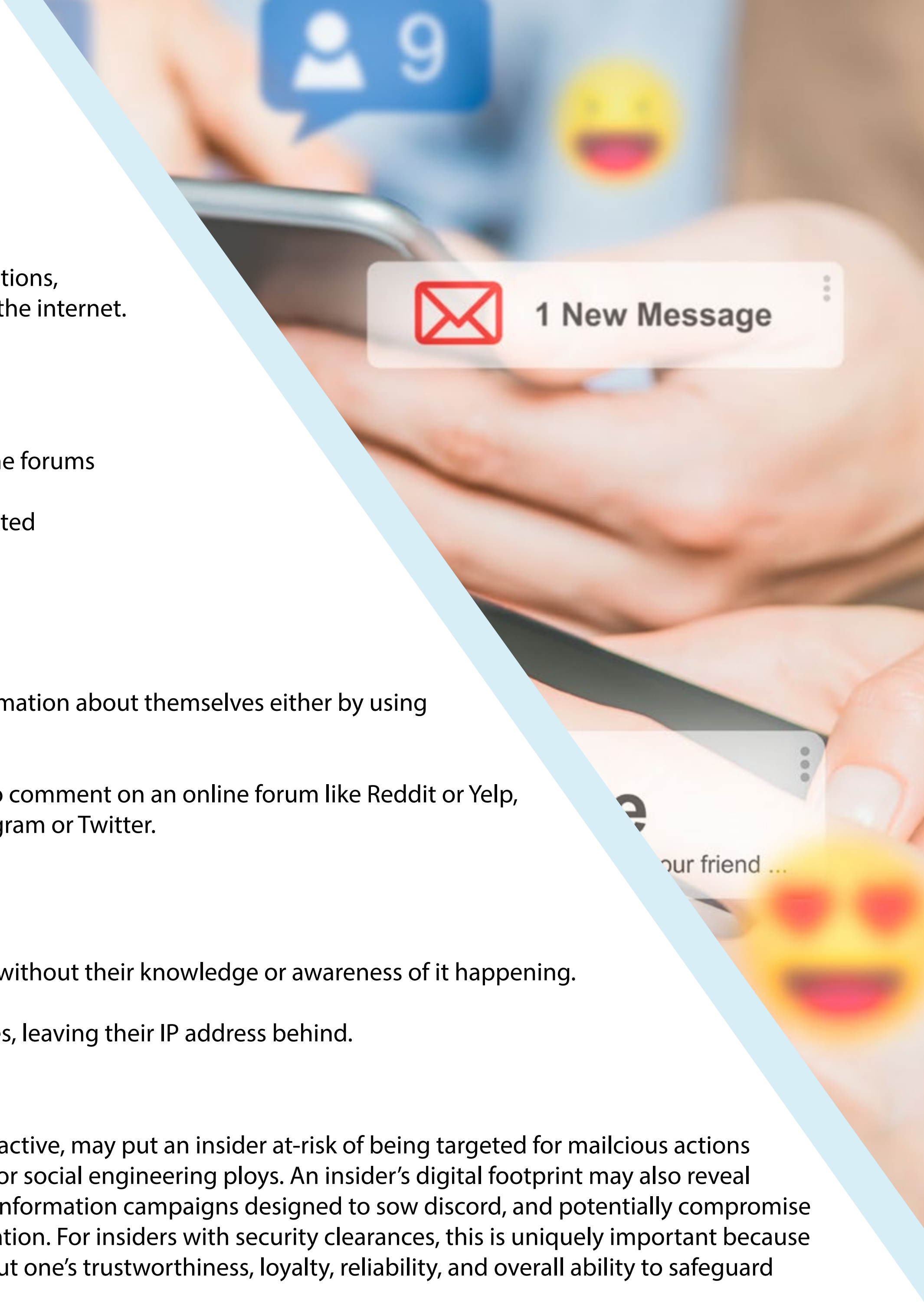
CDSE Center for Development of Security Excellence

JUNE 2022

CONTENTS

Click the individual links to view each topic. You may also use the forward and backward arrows to navigate through each topic in order.

INTRODUCTION



What is a Digital Footprint?

A digital footprint is the unique trail of data pertaining to a user's activities, actions, communications, and transactions on the internet. Examples include:

- Websites visited
- Emails or messages sent
- Information submitted in online forums
- Reviews or comments posted
- Photos and status updates posted

Active Digital Footprint

The user has intentionally shared information about themselves either by using social media sites or other websites.

Example: A user might log into a site to comment on an online forum like Reddit or Yelp, or on social media platforms like Instagram or Twitter.

Passive Digital Footprint

Information is collected form the user without their knowledge or awareness of it happening.

Example: A user visits multiple websites, leaving their IP address behind.

A digital footprint, whether passive or active, may put an insider at-risk of being targeted for mailcious actions such as identity theft, financial scams, or social engineering ploys. An insider's digital footprint may also reveal susceptibility to misinformation or disinformation campaigns designed to sow discord, and potentially compromise an insider's allegiance to their organization. For insiders with security clearances, this is uniquely important because it may reveal information that might put one's trustworthiness, loyalty, reliability, and overall ability to safeguard information into question.

Today around seven-in-ten Americans use social media to connect with one another, engage with news content, share information and entertain themselves. (Pew Research Social Media Factsheet, April 2021)

CHECK YOUR DIGITAL FOOTPRINT

Unsure about your digital footprint? Answer "Yes" or "No" to the questions below, then calculate the total number of "Yes" answers to deterine the complexity of your footprint.

		Y	N
1	Do you make purchases online?		
2	Have you signed up for coupons by creating an account?		
3	Have you registered or subscribed to newsletters or blog updates?		
4	Have you downloaded and used shopping apps?		
5	Have you opened a new credit card account?		
6	Do you use a mobile banking app?		
7	Have you bought or sold stocks?		
8	Have you ever registered your email address with a gym?		
9	Do you receive health care?		
10	Have you ever used apps to track your activities and workouts?		
11	Do you subscribe to an online publication or news source?		
12	Have you ever reposted articles and information you've read?		
13	Do you use social media on your computer or devices?		
14	Do you interact with friends online?		
15	Have you ever shared information, data, and photos with your online connections?		
16	Have you ever joined a dating site or app?		

RESULTS

Yes Answers <5	= A digital footprint that is less complex than most internet users
Yes Answers 5 - 12	= A digital footprint that is average for most internet users
Yes Answers 12+	= A digital footprint that is more complex than most internet users

ASSOCIATED RISKS

Social Engineering

The process of manipulating people into divulging information they shouldn't share or acting in ways they shouldn't act. From the security standpoint, it is using deceptive techniques to influence careless or unwitting insiders into divulging sensitive or classified information and/or breaking normal security procedures. There are various social engineering tactics deployed in cyberspace to target insiders.

Phishing

The practice of sending emails or malicious links, supposedly from reputable sources, to induce individuals to reveal sensitive information such as passwords and credit card numbers. It is a technique employed by malicious insiders or outsiders to exploit victim-insiders. Phishing attacks usually involve a lure, such as the portrayal of a popularor well-respected third party, with a specific request to provide sensitive information. The receiver is lured by the trustworthiness of the third party. Successful phishing attempts have resulted in both identity theft and consumer/customer data breaches.

> *83% of organizations said they experienced a successful email-based phishing attack in 2021, versus 57% in 2020. That equates to a 46% increase in organizations hit with a successful phishing attack last year. (Proofpoint, 2022 State of the Phish Threat Report Feb2022)*

Foreign Collection Methods

Foreign intelligence services may use an individual's (insider's) digital footprint data to understand their pattern of life, preferences, and susceptibilities. Such 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-optees, or agents and non-traditional collectors, can target insiders to collect sensitive or classifed infomation.

Such actors may also pose as industry or market analysts, consultants, job recruiters, bloggers and even journalists. Some examples of contacting an insider to elicit sensitive information may include requests to review and provide comments on draft research papers, including validating data and research techniques, invitations to attend a technical conference or webinar, invitations to an all-expenses paid trip to provide a lecture or workshop, offers to work as a pad consultant, and unsolicited requests to provide clarifications or comments on sensitive or non-public information.

Disinformation Campaign

Occurs when a person, group of people, or entity (threat actor) coordinate to distribute false or misleading information while concealing the true objectives of the campaign. Adversaries and threat actors may aggregate and research digital footprint data to customize content that is then used to target social media platform users to draw their attention, and amplify and spread disinformation.

Radicalization Along the Pathway to Violence

Domestic Violent Extremists and Foreign Terrorist Organizations exploit a variety of popular social media platforms, smaller websites with targeted audiences, and encrypted chat applications to recruit new adherents, plan and rally support for in-person actions, and disseminate materials that contribute to radicalization and mobilization to violence. Similarly, many indicators of an attack or violent extremist travel may be observed in online forums or on social media. This may include communicating intent to engage in violence or a direct threat with justification for action; or communicating directly with or seeking to develop a relatnioship with violent extremists, or being contacted directly by them.

HOW TO PROTECT YOUR DIGITAL FOOTPRINT

Limit shared information on social media.

Tighten up privacy settings on social media.

Limit the amount of data placed on the internet.

Occasionally clean browser cookies, and other tracking files on your personal devices.

Do not open attachments or access links from unknown or questionable sources.

HOW TO PROTECT YOUR DIGITAL FOOTPRINT

Use VPN services, if and when possible.

Anonymize, disallow, or restrict location access of tracking by applications.

Install and keep antivirus software updated on personal devices.

Periodically review both financial/credit and medical/health information.

Setup credit reporting notifcations.

Continually update passwords and password protections, especially after being informed of a data breach.

HOW TO PREVENT, DETECT, DETER AND MITIGATE AN INSIDER COMPROMISED BY SOCIAL ENGINEERING

Insider Threat Programs

Peers, co-workers, friends, and family members can observe when an insiders' behavior becomes concerning. The same is true for online interactions. Reporting concerning behaviors, to include threats of violence over the internet, to an organization's insider threat program can help prevent harm from occurring to the insider, others, or the organization. Additionally, self-reporting of potential targeting by foreign adversaries, or falling prey to a phishing attempt, can help the security program manage threats to the organization.

Vetting

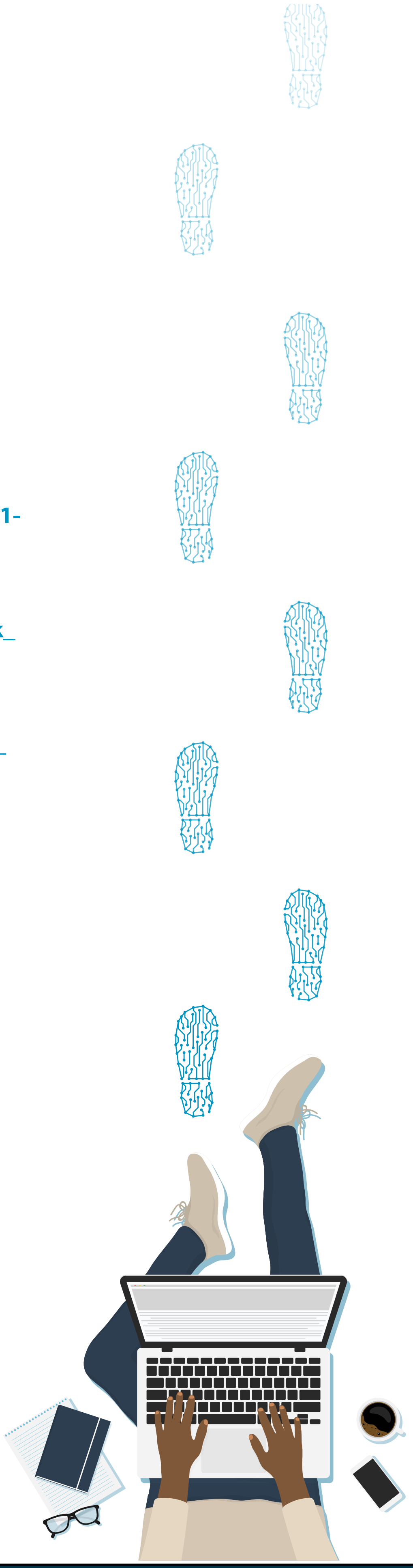
Human Resources and Personnel Security both play a vital role in preventing insiders who are compromised from earning or maintaining positions of trust. The inclusion of social media into the hiring process and continuous evaluation (for cleared individuals), can provide insight into an insider's substance abuse, allegiance, criminal conduct, foreign influence, foreign preference, and foreign travel.

For cleared employees, federal agencies can collect social media information in the personnel security background investigations, as long as the information pertains to adjudicated guidelines, per Security Executive Agent Directive 5.

Training and Awareness

Providing training and awareness materials to the workforce can help deter unwitting and witting insiders from becoming threats. For examples, see the Additional Resources on the next page.

ADDITIONAL RESOURCES



Applied Research on Social Media and Security (Webinar):
https://cdse.acms.com/pnk8ulukyrgi

Cyber Insider Threat (eLearning Course):
https://www.cdse.edu/Training/eLearning/INT280/

Cybersecurity Attacks - The Insider Threat (Short):
https://securityawareness.dcsa.mil/cdse/multimedia/shorts/insider-threat/story_html5.html

Cybersecurity Awareness (eLearning Course):
https://www.cdse.edu/Training/eLearning/CS130/

Potential Risk Indicators: Insider Threat (Job Aid):
https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf

Facebook Smartcard:
https://www.cdse.edu/Portals/124/Documents/jobaids/cyber/Facebook_Social_Networking_Site_Configuration_Guide.pdf

LinkedIn Smartcard:
https://www.cdse.edu/Portals/124/Documents/jobaids/cyber/LinkedIn_Smartcard_Trifold.pdf

Twitter Smartcard:
https://www.cdse.edu/Portals/124/Documents/jobaids/cyber/Twitter_Social_Networking_Site_Configuration_Guide.pdf

Your Evolving Digital Life (Webinar):
https://www.cdse.acms.com/p1a4p3e6flx/