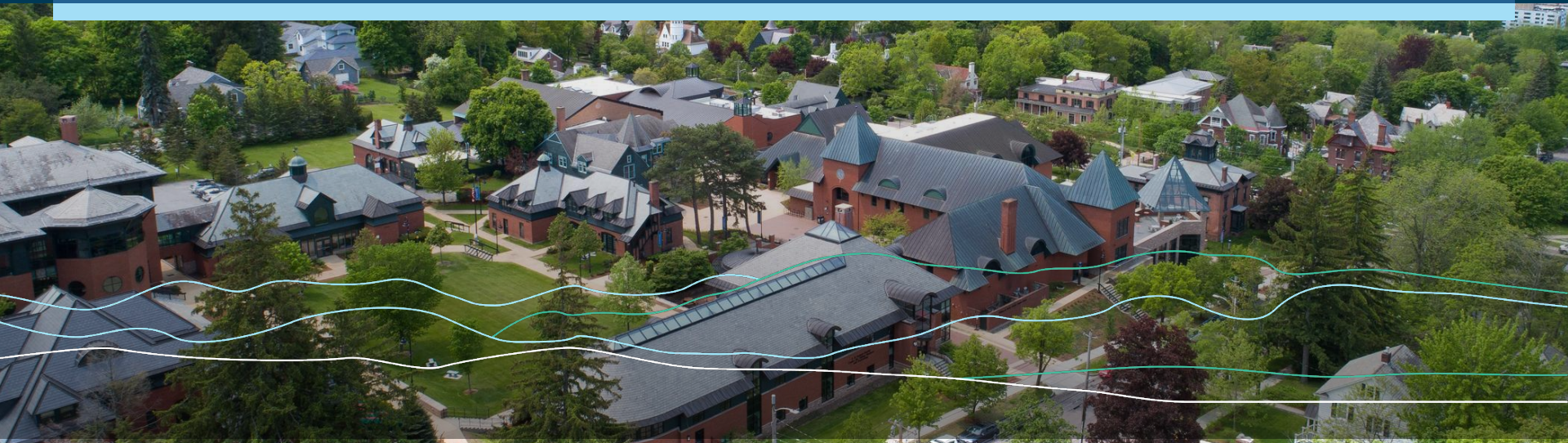
CHAMPLAIN COLLEGE

Mod 4 - Human Factors in Cybersecurity and Bias

SEC-110



What is Bias?

Definition: Prejudice in favor of or against one thing, person, or group compared with another, usually in an unfair way.

Examples:

- Assuming a person who is bad at sports is also bad at academics, even without evidence to support it.
- Focusing only on information that supports your existing beliefs and ignoring other perspectives.
- An individual actively avoiding another based on one negative trait.

Bias in Cybersecurity?

Why is it important to consider bias in relation to cybersecurity and information assurance?

Lots of Reasons - including:

- Decision Making
- Risk Management
- Technical approaches
- Resource allocation
- Diversity of perspectives

Bias in the News

Bias is everywhere we look, even in places we think we can trust. News outlets will let their own personal bias and experiences **cloud their judgement** of what is objectively occurring.

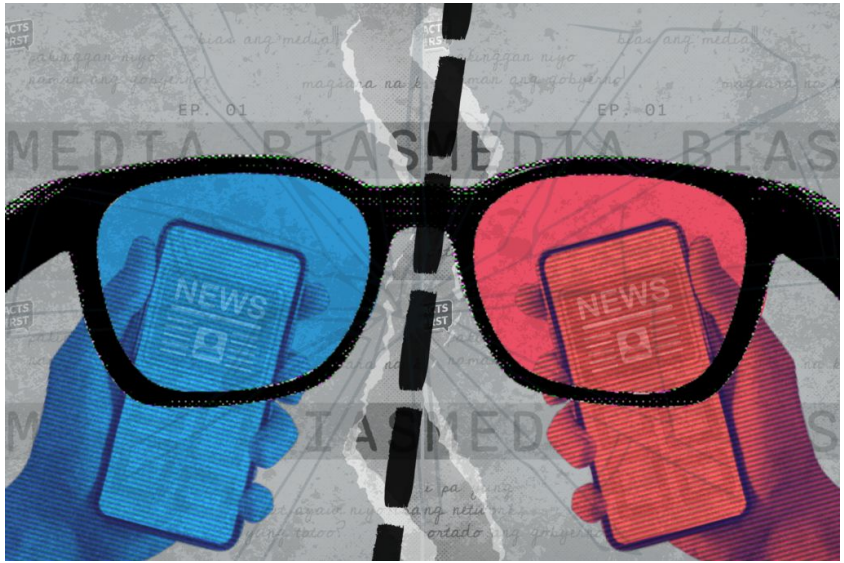
Example:

Two news outlets reporting on the same news story with **different** views/opinions on what happened.

Media Bias

What is Media Bias?

Media bias occurs when news outlets or other forms of media present information in a way that supports a particular viewpoint, rather than presenting all sides of an issue fairly.



How to combat Media Bias?

How to combat Media Bias:

- **Process** before sharing.
- Check **authenticity** of your source.
- Is the source from an **expert** in their field?
- Evaluate the **purpose** of your source. Is it meant to persuade, inform, or mislead?

A Little Bit on Bias

Decision Quality is critical for cybersecurity.

Basically - what are the steps to making a good decision?

- Meeting Goals
- Logical Thinking
- Forecasting (Thinking Ahead)
- Risk Assessment
- Evaluation

Can these be influenced by biases?

Cognitive Bias

When individuals tend to **act unreasonable or irrational** when thinking in an organized way.

Example:

Thinking that taking a plane is more dangerous than driving/traveling in a car.

Types of Cognitive Biases

- Media Bias
- Motivational Bias
- Nonverbal Bias
- Affinity Bias
- Halo/Horns Effect
- Similarity Bias
- Contrast Effect
- Attribution Bias
- Confirmation Bias
- Appearance Bias
- Conformity Bias

Motivation Bias

Occurs when someone's personal motivations, desires, or interests influence their thoughts, decisions, or perceptions in a way that leads to biased conclusions.

Example:

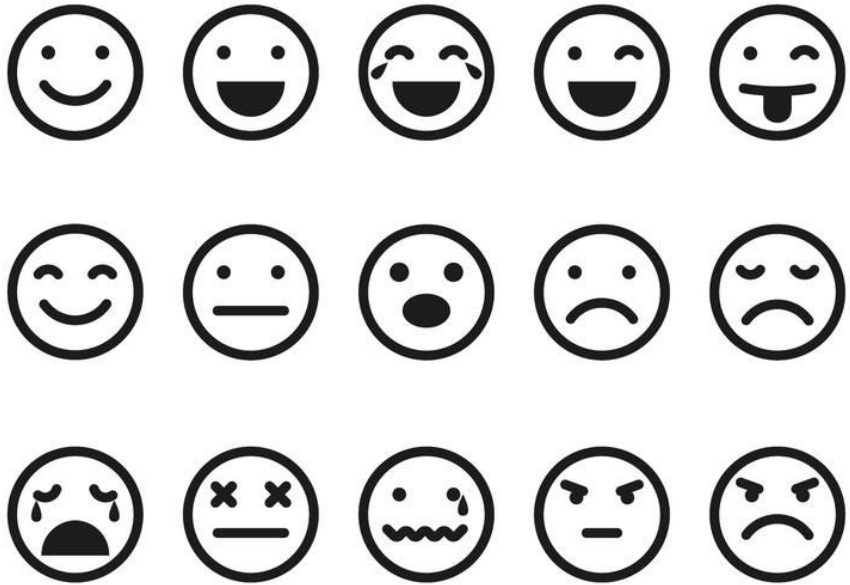
A common example of motivational bias in cybersecurity is when security teams downplay or dismiss a vulnerability because they conflict with existing beliefs about their network's security posture.

Nonverbal Bias

Occurs when people show positive or negative behavior towards another group, ultimately excluding others.

Example:

A junior analyst raises concerns about suspicious network activity, but senior staff dismiss them with eye rolls and crossed arms because the analyst "looks young."



Affinity Bias

Seen when two or more people are drawn together through a **common connection** like a shared hometown, hobbies, or attending the same school.

Example: Security team overlooks suspicious behavior from a colleague who attended the same university, shares similar hobbies, or is part of their social circle. Because of this, an insider threat goes undetected longer when perpetrators are well-liked or socially similar to security staff

Halo / Horns Effect

A form of bias in which someone allows their opinions of a person to be formed around **any given action** from that person.

Halo Effect

A pentester with certifications is assumed to be great at ALL security domains. The team doesn't review their cloud security recommendations even though their expertise is in network penetration. Poor security architecture decisions were made because nobody challenges the "expert"

Horns Effect

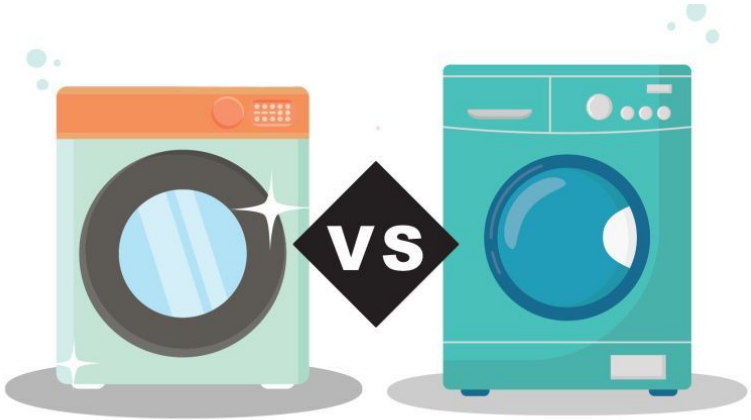
A company experiences a data breach, but responds by adding more comprehensive security improvements. Despite their efforts, they are still viewed as "insecure" years later. Any security related news about them gets amplified. Their improved security posture is ignored because the past breach defines them.

Contrast Effect

Comes from **comparing** those around us to what we believe is a **general stereotype** for their type of work, rather than off of their skills in the given line of work.

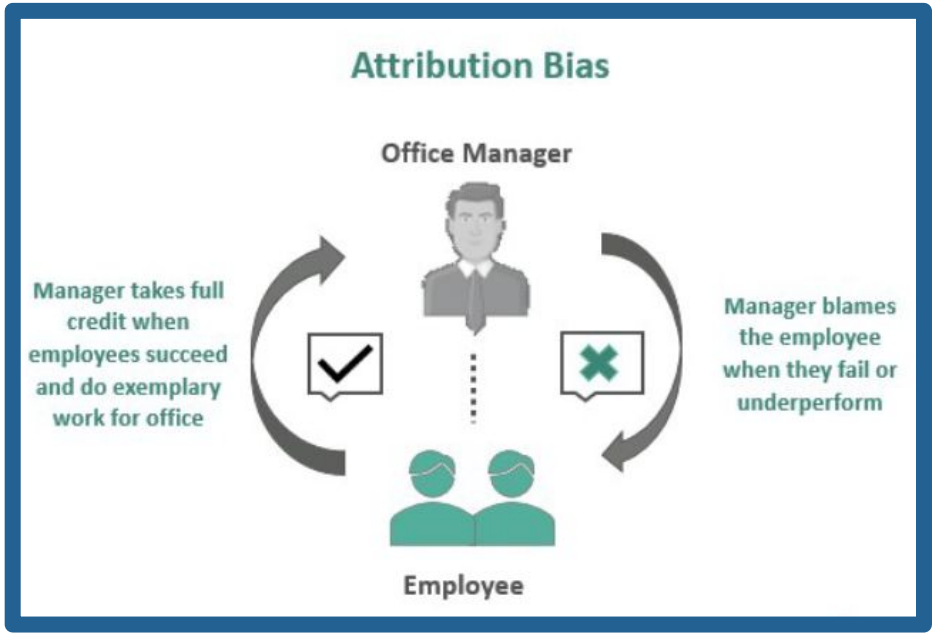
Example:

After responding to a massive ransomware attack, the team receives an alert about credential stuffing attempts. Team dismisses it as "not a big deal" because compared to ransomware, it seems minor. But, in reality, credential stuffing could lead to account compromise and data exfiltration.



Attribution Bias

Attributing a success or loss to **external factors** that occurred.



Example:

An organization experiences a data breach where the attackers achieved network access through a misconfiguration in a vendor application. The organization blames the vendor. However, the configuration setting missed had been disabled by someone in their organization.

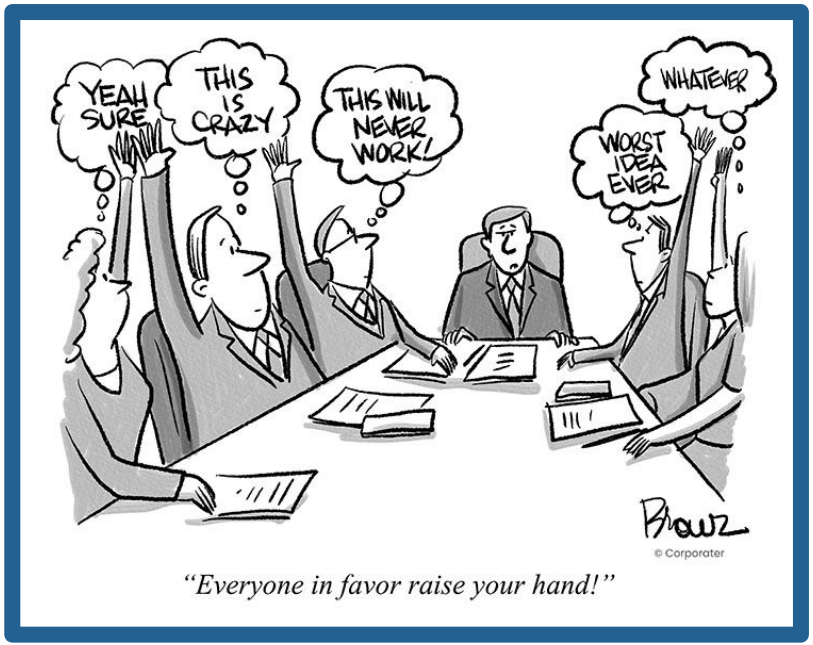
Confirmation Bias

After making a judgement call, it is human nature to look for or interpret new information such that it **supports their prior beliefs**, causing tunnel vision.

Example:

Our security information and event management (SIEM) tool has a rule that generates many false positive alerts. Because of the number of alerts, the analyst stops investigating alerts from that rule altogether. One day the alert IS a real incident, but the analyst dismisses it based on historical pattern. The incident escalates and results in a data breach.

Conformity Bias



Seen when an opinion is made only to **conform with a group-think mentality**, or for fear of speaking out against a group.

Example:

The security team is reviewing a pen test report that has a critical finding. The most senior person on the team looks around the room and says, "This isn't realistic. Our Web Application Firewall (WAF) would block this. Raise your hand if you agree." All of the junior analysts raise their hand, although several disagree.

Human Factors and Why They Matter

Humans are the biggest threat to cybersecurity

Most cyber attacks happen not because of technical flaws, but because people are tricked.

- Clicking suspicious links
- Using the same password everywhere
- Leaving passwords on sticky notes

What is Social Engineering?

Social Engineering is manipulating people into giving up confidential information or performing actions that compromise security.

Common Techniques

Phishing

- a scam where attackers deceive people into revealing sensitive information or installing malware
- Spear Phishing: sending fraud emails from a known sender to targeted individuals
- Whaling: Targeting high-level executives with phishing attacks.

Vishing

- (Voice Phishing): using phone calls or voice message to deceive victims into revealing information

Common Techniques

Pretexting

- An attacker fabricates a story/text to deceive a victim into providing sensitive information.

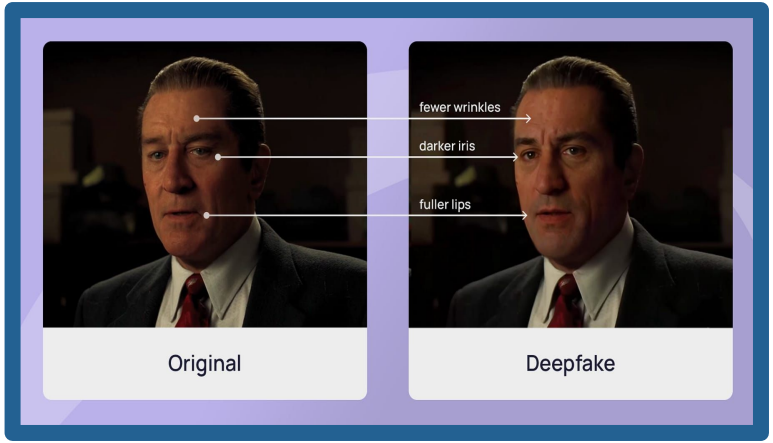
Jeff Bezos/Twitter

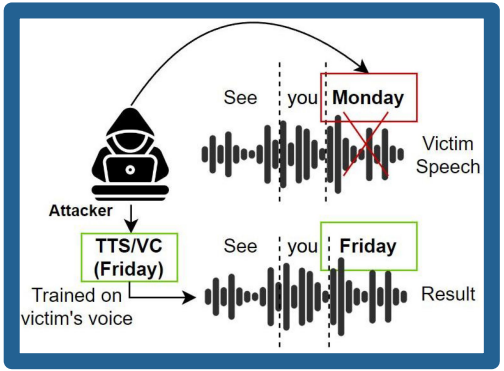
Baiting

- Physical Baiting: an attacker leaves a malware-infected USB drive in a high traffic location, hoping an employee will pick them up and plug them into their computer.

Deepfakes

- **Deep Fakes:** altered text, audio, images, or videos meant to make it seem like a person did something they never did.
  - Using synthetic audio to impersonate a CEO asking their employee for money over the phone.
  - Defacing a person or organization by making them appear to do or say something controversial.





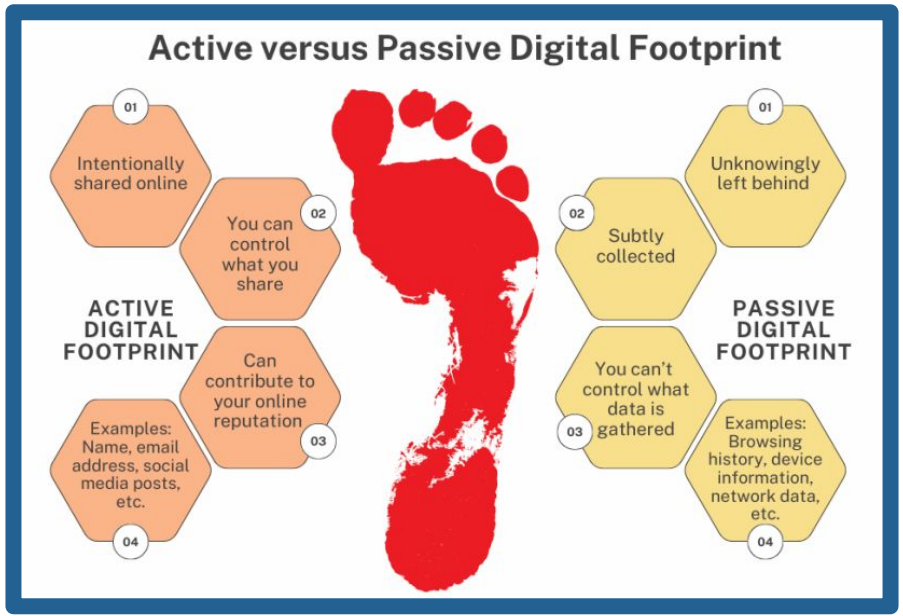
Intro to OSINT

Open **S**ource **INT**elligence: The process of collecting and analyzing publicly available information to generate actionable intelligence

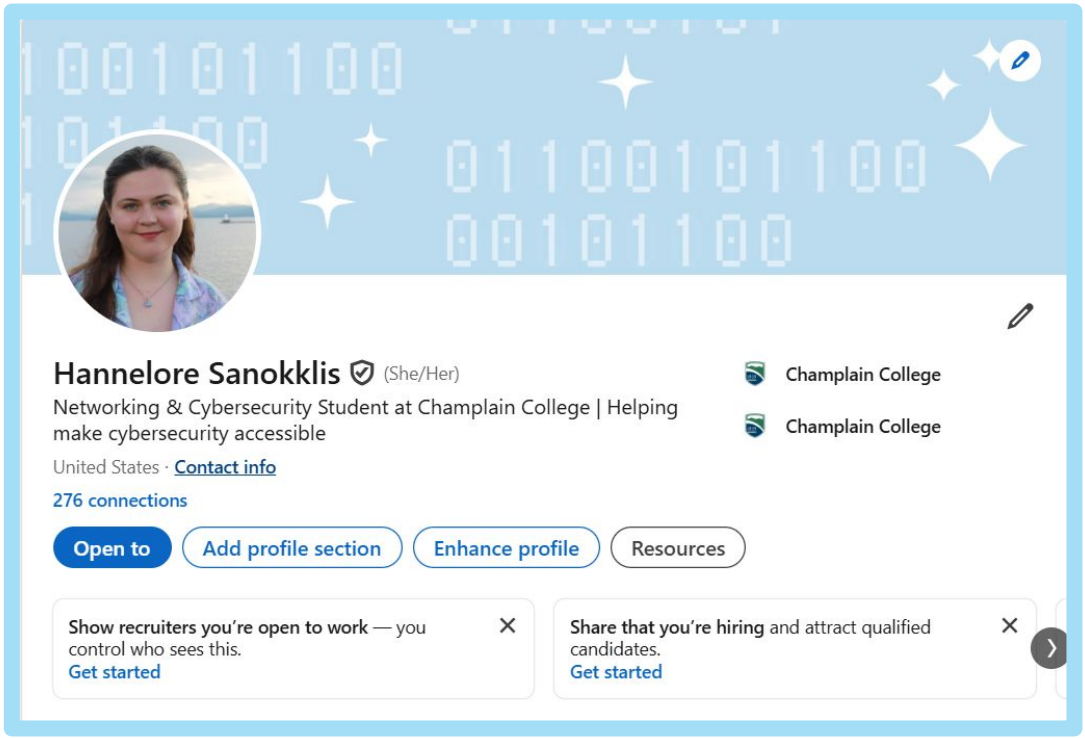
- **Sources of OSINT:**
- Websites
- Blogs
- Social Media
- **Purpose in CyberSec:**
- Recon during pen testing
- Attacker profiling
- Threat intelligence

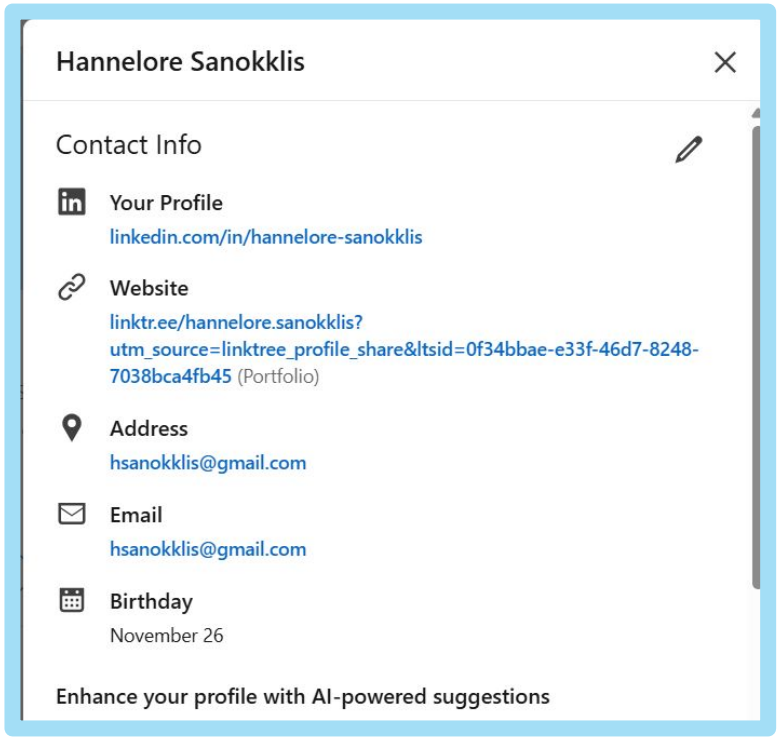
OSINT and Digital Footprint

The more you put out about yourself online, the easier it is for a malicious actor to social engineer you.

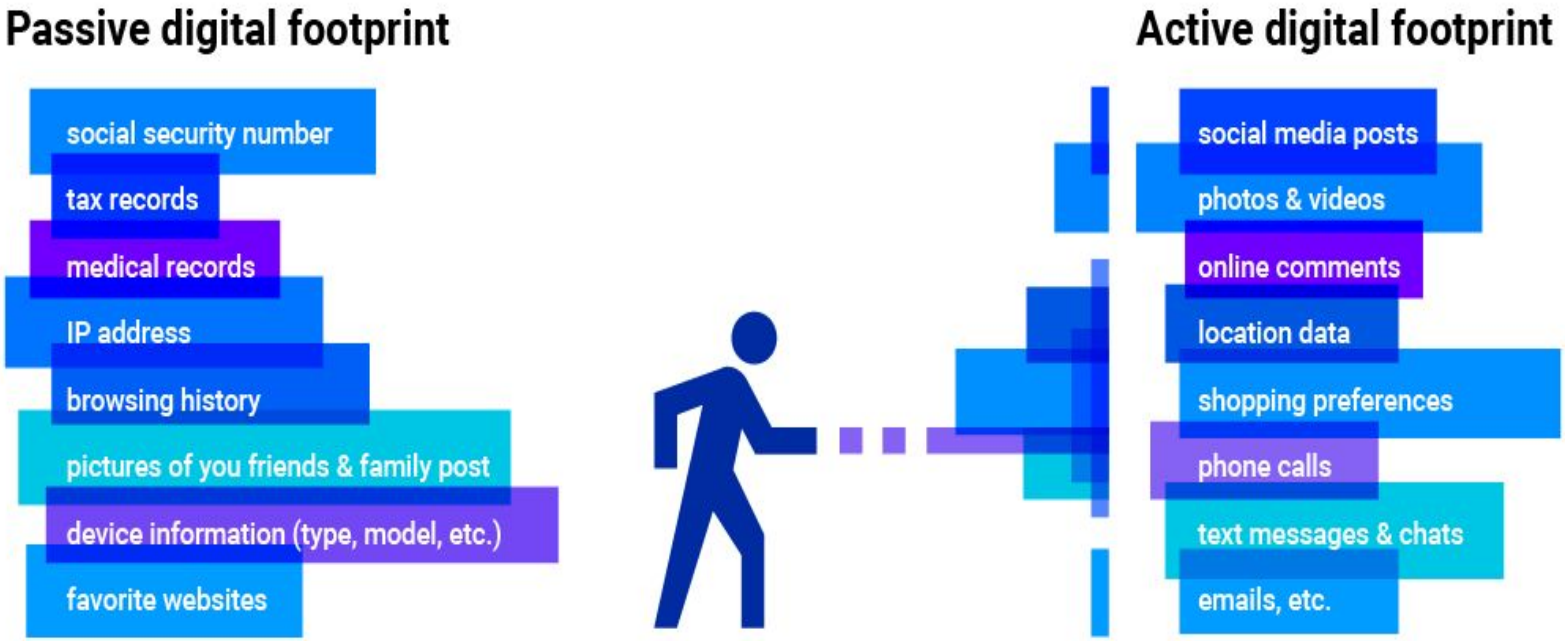


Digital Footprint Example



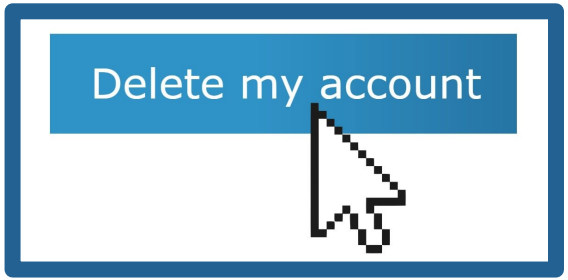


Digital Footprint Example



Cleaning Your Digital Footprint

- **Google Yourself**
  - Check name/usernames
- **Delete/deactivate old accounts;**
  - https://backgroundchecks.org/justdeleteme/
  - Online Stores
  - Apps
- **Clear out social media**
- **Unsubscribe from emails/newsletters**
- **Revoke app permissions**
- **Check is passwords/emails have been compromised;**
  - https://haveibeenpwned.com/



Social Engineering Toolkit (SET)

The Social Engineering Toolkit is an open-source tool focused on penetration testing involving Social-Engineering.

- **Key features:**
  - Spear phishing attack vector
  - Website attack vectors
  - Infectious media generator
  - Credential harvester

BeEF (Browser Exploitation Framework)

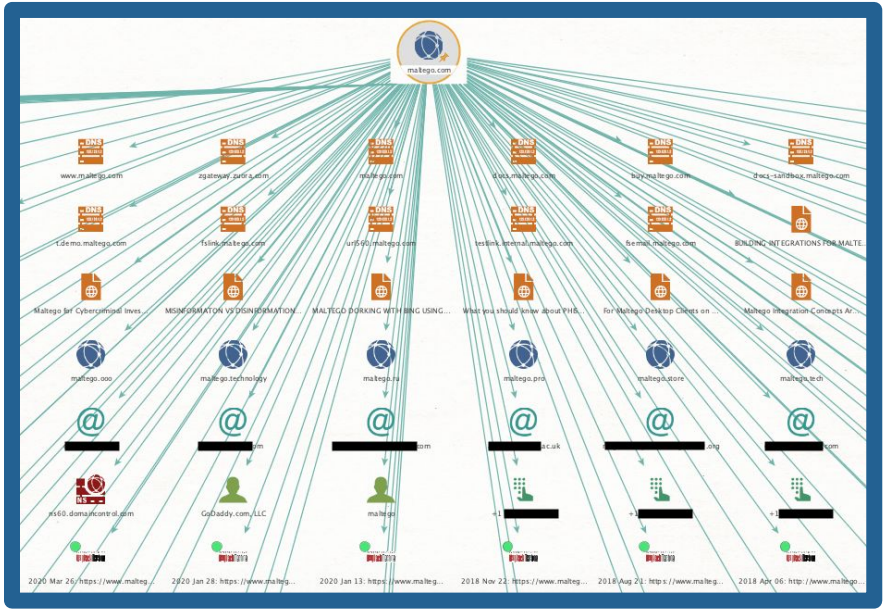
BeEF is a penetration tool that mainly focuses on the web browser. It allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors.

- **Key features:**
  - **Exploiting Vulnerabilities in Web Browsers**
  - **Client-Side Testing**
  - **Real Time Interaction**
  - **Education & Training**
  - **Cross-Site Scripting (XSS) Exploitation**

Maltego

Maltego is a cyber investigation platform that is used in gathering and visually displaying information.

- It can be used for OSINT and Threat Intelligence.
- It can also automate repetitive processes which saves an investigator's time.



Real World Example

- **In 2016, the U.S. Department of Justice (DOJ) experienced a data breach due to a social engineering attack.**
  - A hacker posed as a new DOJ staff member and called the department to obtain the code for the DOJ intranet.
  - The hacker was able to use this code to infiltrate internal systems and obtain about 200GB of data (contact details of FBI and other government employees).

Mitigation and Best Practices

- **Think before you click**
- **Use strong and varying passwords**
- **Multi-Factor Authentication (MFA)**
- **Keep your systems up to date**
- **Social engineering training**
- **Be skeptical!**