Cybersecurity Landscape

Content

- Cybersecurity
- How does cybersecurity work?
  Challenges of Cybersecurity
- Cybersecurity trends
- Common Cyberattacks and Solutions
- ITAM v/s CSAM
- Cybersecurity Asset Management
- Case Study

Cybersecurity

- Cybersecurity is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals.
- companies should be protected against
    - phishing schemes
    - ransomware attacks
    - identity theft
    - data breaches
    - financial losses

Why is Cybersecurity Important?

- personal information of millions of people
- strong financial impact
- loss of the trust of customers

According to Cybercrime Magazine, cybercrime will cost the world $10.5 trillion annually by 2025!
Furthermore, global cybercrime costs are predicted to rise by almost 15 percent yearly over the next four years.

Live Cyber Threat Map

How Does Cyber Security Work? The Challenges of Cyber Security

Application Security

- defend organization’s software and services
- write secure code,
- design secure application architectures,
- implement robust data input validation

Cloud Security

- creating secure cloud architectures and applications

Identity Management and Data Security

- authorization and authentication of legitimate individuals
- powerful information storage mechanisms

Mobile Security

- information on mobile devices like tablets, cell phones, and laptops
- unauthorized access, device loss or theft, malware, viruses, etc.

Network Security

- protect network and infrastructure from disruptions, unauthorized access

Disaster Recovery and Business Continuity Planning

- massive power outages, fires, natural disasters
- resuming and recovering lost operations and systems

User Education

Cybersecurity Trends

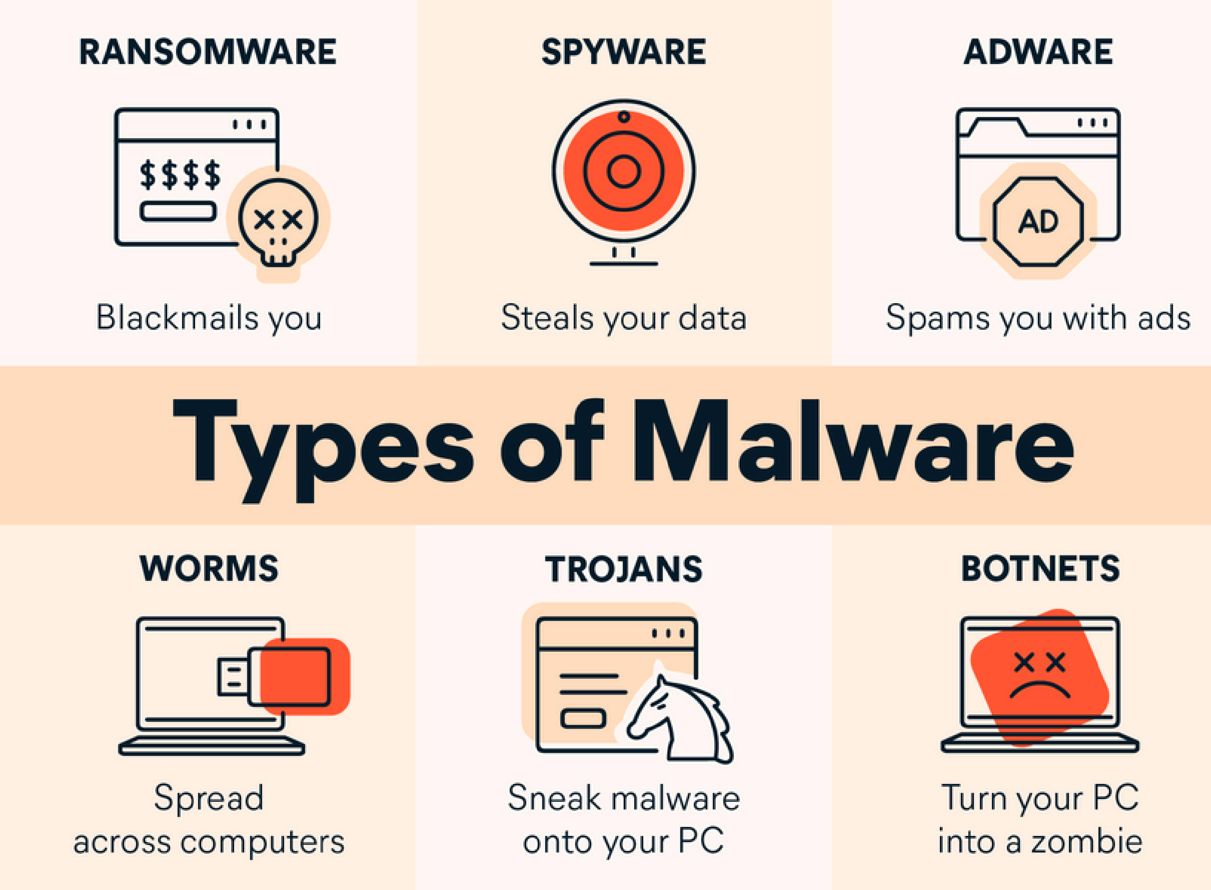
1. Automotive Hacking is on the Rise
2. Artificial Intelligence's Potential (AI)
3. The New Target is Mobile
4. Data Breach: A High-priority Target
5. Technology and Risks in a New Era: IoT on a 5G Network
6. Ransomware with a Specific Target
7. Cyber Warfare Supported by the Government
8. The Cloud May be Vulnerable as Well
9. Threats from Within
10. Cybersecurity mesh

Common Cyberattacks and Solutions

1. Malware:

Code with maleceous intent that steals data destroy something on computer
Occur due to OS vulnerabilities, downloading illegitimate software, compromised email attachment

- Trojan: Disguises as legitimate software or is included in legitimate software, create backdoors in security to let other malwares in
- Viruses: Attach themselves to clean files and infect them, spread uncontrollably, damaging system core functionality, deleting or corrupting files, appear as executable files that you can download from the internet
- Worms: infect entire networks/devices, uses infected machine to infect more
- Botnets: network of infected computers, work under control of an attacker
- Spywares
- Ransomware: Denies access to files, demands ransom



1. Avoid clicking on links or attachments from unknown senders
2. Robust and updated firewall
3. Updated OS and software programs

2. Phishing

- Performed via email
- Click on a link and enter personal data
- Mimic banks, credit cards, companies, businesses like amazon, flipcart

Steps performed in phishing:

1. Planning
2. Setup Phase
3. Execute the attack
4. Records the information
5. Identity theft and fraud

- Beware of how phishing emails work
- Check the sender email address
- Look out for common generalized addressing eg. Dear client
- Always hover over links to check the redirect address

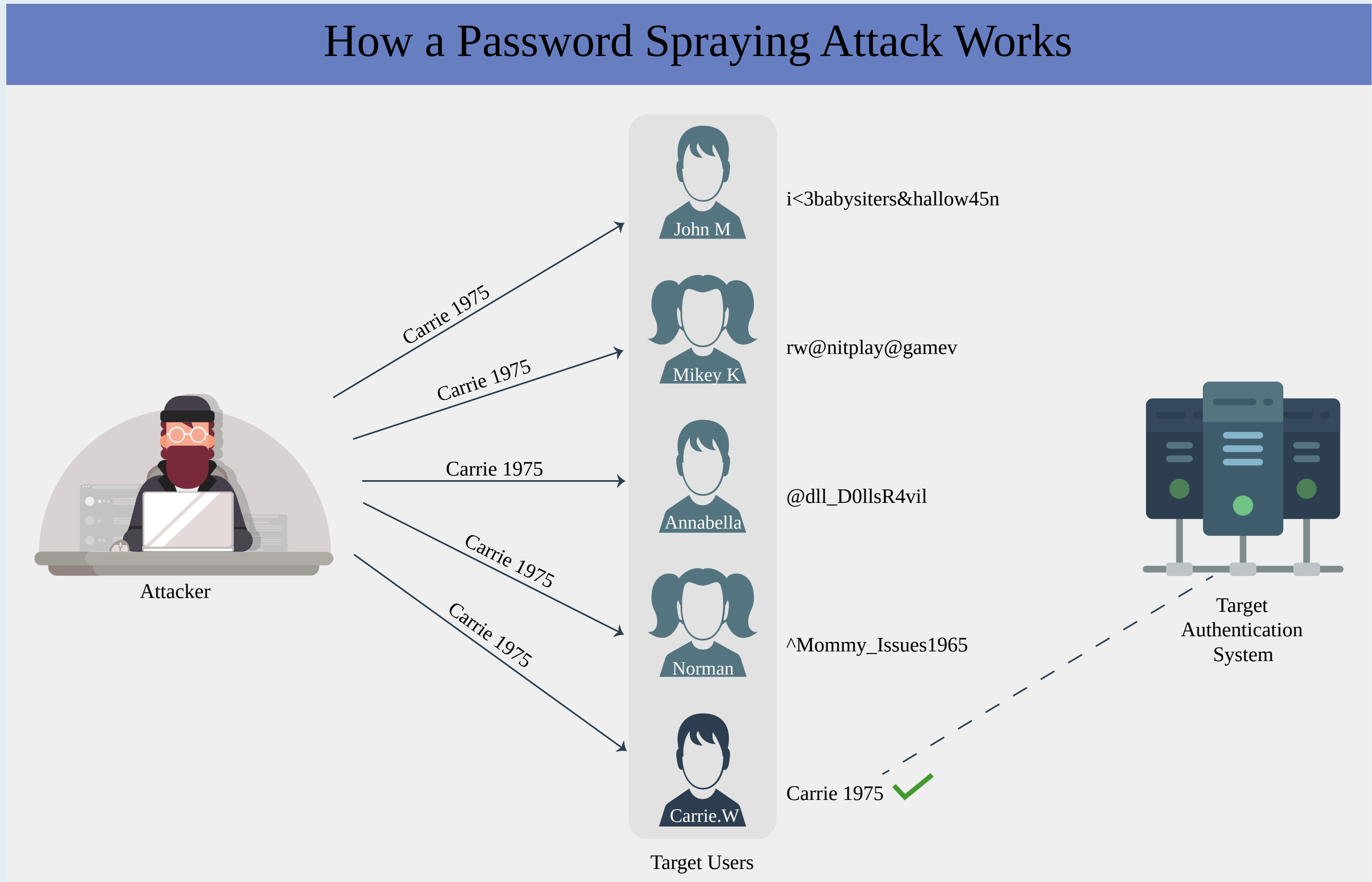
3. Password Attacks

- Attempt to obtain or decrypt a users password for illegal use
- Hackers can use cracking programs, dictionary attacks and password sniffers in password attack

Types of Password Attacks:

1. Brute Force Attack: Computer program to try possible password combinations, Large proportion of key space is searched systematically
2. Dictionary attacks: Program or script, tries only those possiblities which are most likely to succeed
3. Keylogger attacks: Program to track all of user's keystrokes, malware should be installed in users device, stronger passwords don't provide much protection

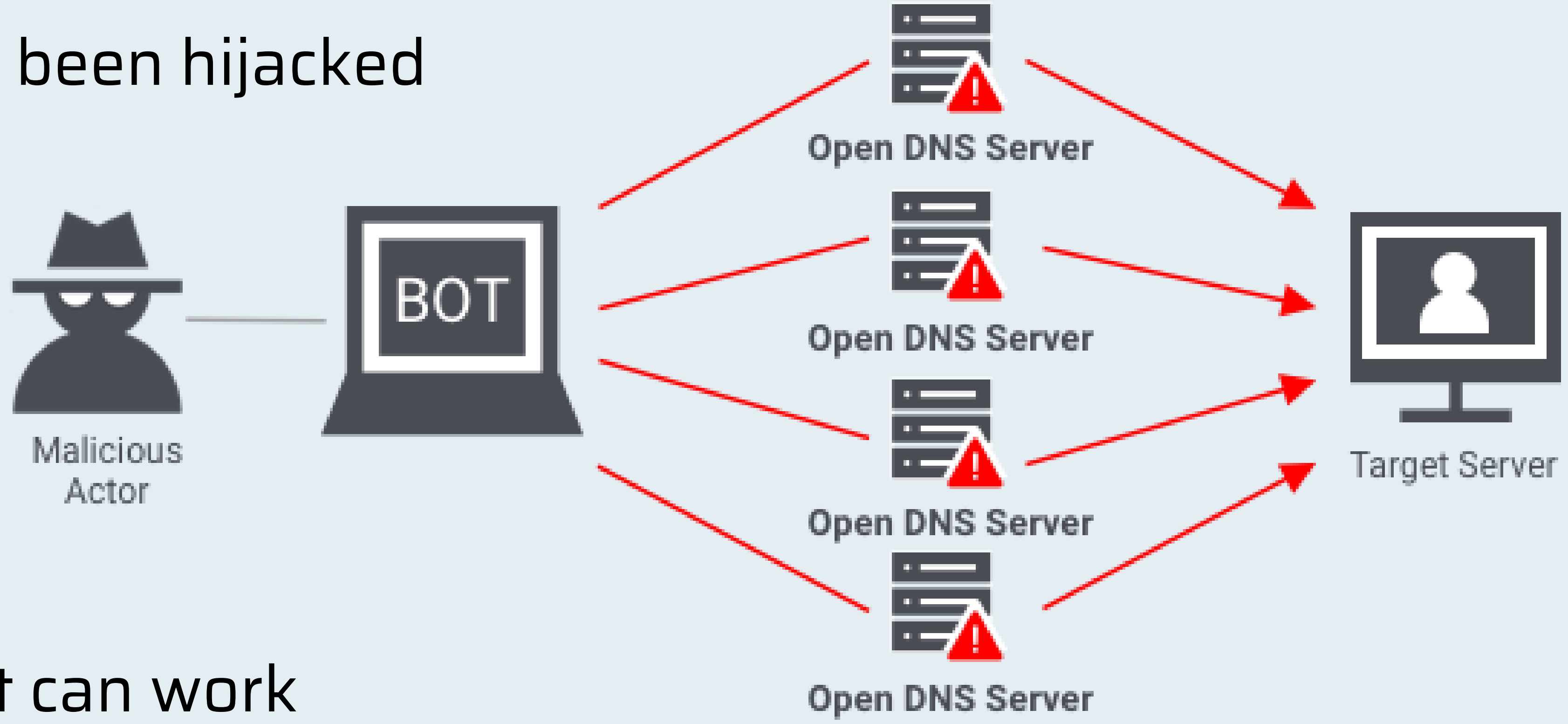
- Practice best practices about passwords
- Alphanumerics, update, common passwords should not be used


How a Password Spraying Attack Works

4. DDOS Attacks

- **DOS Attack:**
- Attackers send high volume of data through the network until it becomes overloaded and can no longer function
- **DDOS involves multiple computers**
- Person may not even realize that his or her computer has been hijacked

- Keep system as secure as possible
- Regular software updates
- online security monitoring
- Monitoring data flow to identify unusual spikes in traffic
- Due diligence in physically monitoring connections
- Dislodging a plug that connects website server to internet can work



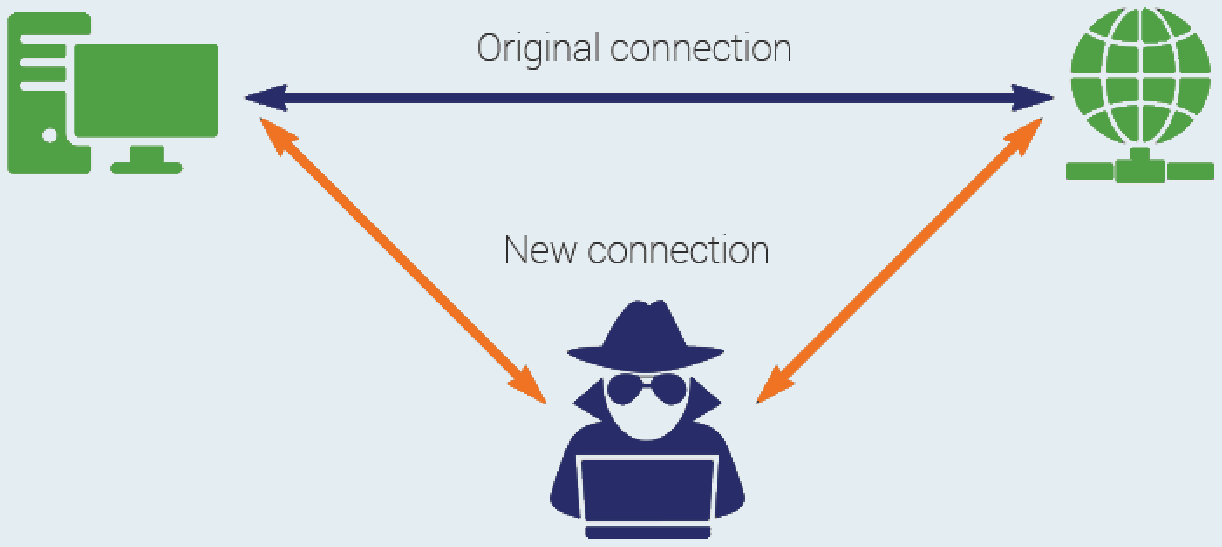
In 2018, GitHub was hit by the then-largest-ever DDoS attack, which flooded their servers with over 120 million data packets every second.

5. Man in the Middle Attack:

- By impersonating the end points in online information exchange
- For eg: Banking online - Man in the middle communicate with you by impersonating the bank and with bank by impersonating you.

- Gains access through non encrypted wireless access point - one that doesn't use WEP, WPA or other security measures
- Gain information by spoofing Address Resolution Protocol (Protocol used when you are connecting gateway from your computer)

- Use encrypted WAP (Wireless Access Points)
- Check security of your connection
- Investing in a virtual Private Network(VPN) which spoofs your entire IP address



Man in the middle, Phisher, or annonymous proxy

6. Drive-by Download:

- Opening a compromised web-page/ Accepting any software download
- Take advantage of a browser or app or OS that is out of date and has security flaws

- Avoid visiting web sites that could be considered dangerous or malicious
- Use a safe search protocol
- keep OS and internet browser up to date
- Use comprehensive security software

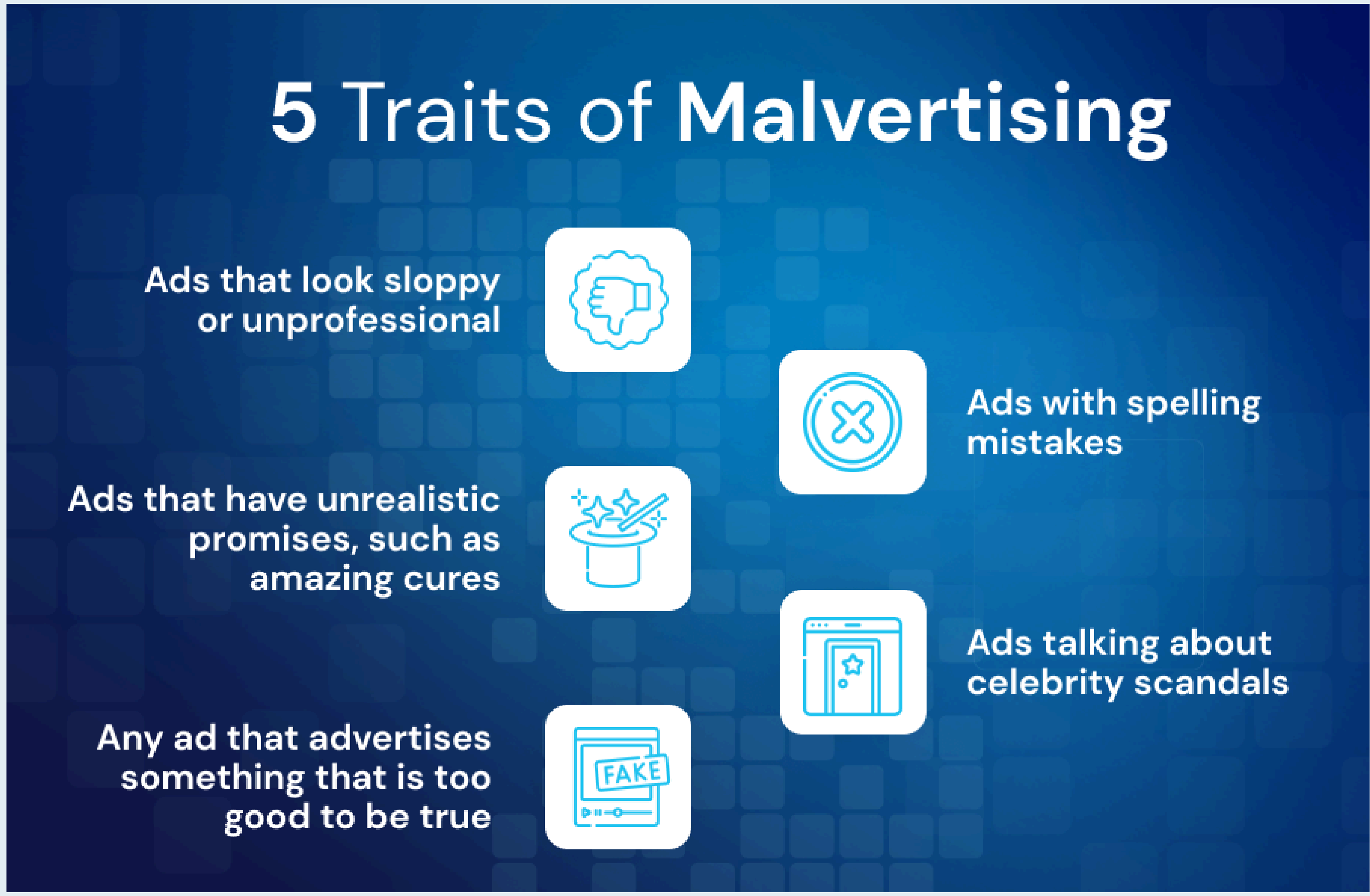
7. Malwartising:

- Criminally controlled advertisements which intentionally infect people and businesses
- Any ad on any site
- Doesn't need a new browser window so you will not know about this
- Redirected to some criminal server, malware injection, infected system

- Use an ad-blocker
- Have ad-blocker extensions installed on browser
- Regular software updates of browser
- Use common sense

8. Rogue Software:

- Form of malicious software and fraud
- Misleads users into believing that there is a virus in their computers
- Manipulates them into paying money for a fake malware removal tool
- Form of scareware manipulates users through fear



5 Traits of Malvertising

Ads that look sloppy or unprofessional

Ads with spelling mistakes

Ads that have unrealistic promises, such as amazing cures

Ads talking about celebrity scandals

Any ad that advertises something that is too good to be true

- Ads offering free or trail version of security programs
- Encouraging purchase of deluxe versions
- Pop-up warnings that computer is infected
- Steal information, slow down computer, corrupt files, disable updates for antivirus software, prevent from visiting security
- Updated firewall, install good antivirus, general level of distrust on internet

IT Asset Management vs. Cybersecurity Asset Management

How is IT asset management different from cybersecurity asset management?

- IT Asset Management is about managing assets to optimize spend and efficiency.
- Cybersecurity asset management is about understanding all of your assets to strengthen your company's cyber risk posture.

What is IT Asset Management (ITAM)?

financial, licensing, and contractual aspects of IT assets

Key aspects:

Hardware asset management
Software asset management
Licensing and compliance

With the rise of cloud computing, and the adoption of SaaS platforms, it’s harder than ever before to account for — and manage — all hardware and software assets.

IT Asset Management vs. Cybersecurity Asset Management

What is Cybersecurity Asset Management?

Cybersecurity asset management is the process of gathering asset data to strengthen core security functions, including:

- Detection and response
- Vulnerability management
- Cloud security
- Incident response
- Continuous control monitoring

Similarities between ITAM & Cybersecurity Asset Management

- Up to date asset Inventory
- asset inventories are managed by CMDB's

The Differences Between ITAM & Cybersecurity Asset Management

CSAM need to answer critical questions, like:

- Are devices running the latest software versions?
- Are all devices covered by security controls?
- Are devices vulnerable?

Cybersecurity Asset Management

Identifying any security gaps

- vulnerable computers with outdated software
- unknown or forgotten assets
- assets that have reached end-of-life, etc

The benefits of effective Cybersecurity Asset Management include:

- Discover unknown assets
- Mitigate security threats
- Compliance
- Manage risk
- Improved productivity through reduced downtime
- Reduced costs

Cybersecurity Asset Management Approach

- Asset discovery
- Asset inventory
- Asset visibility
- Configuration management database (CMDB)
- Restricting assets

Cybersecurity Asset Management

Cybersecurity Best Practices for your Organization

- Multi-factor authentication: verifying a user's identity with two or more independent credentials by using an app or pushing notifications to another device. It is also important to not to have duplicate passwords for work and personal logins. The recommended time frame to change your password is about every 90 days.
- Phishing and training: train your employees to identify any types of phishing emails and red flags through security training and regular testing.
- Endpoint security: protecting your endpoints (desktops, laptops, servers, etc.) with monitoring and remediation.
- Vulnerability assessments: vulnerability scanning will quickly scan, identify, and patch any vulnerabilities found within your organization's endpoints.
- Incident response: it's not if, but when an attack will happen. Having a documented response plan will save time and money when said incident occurs.

In the world of cybersecurity, you simply cannot secure something if you don't know it exists.
Your organization is only as strong as your weakest link.
That is why cybersecurity asset management is a critical component for your company.

Case Study

Lionbridge powers strong Security Program with Axonius.
Lionbridge provides translation, content creation and localization solutions in 350+ languages.
Maintains solution centers in 26 countries.

Key challenges:
Getting accurate and quick answers to asset-related questions, maintaining an up-to-date asset inventory, and ensuring security control coverage

Solution:
Axonius Cybersecurity Asset Management Platform

- Seeking Asset Visibility
- Taking Action With Axonius
- A Powerful Incident Response Tool
- Transcending Beyond a Security Tool
- Staying Ahead of Cyber Attackers

Thank You