Case 1: Backdoors

The Goal of Backdoors:
Backdoors are created to bypass security measures and gain unauthorized access to systems. Attackers use them to steal data, install malware, or maintain ongoing access to launch future attacks. The real danger lies in how hidden and persistent these methods can be, making detection hard.

Who Would Be a Target?
Backdoors target companies, governments, or individuals with valuable data or access. Like corporations with intellectual property, government systems holding sensitive information, or even personal devices linked to critical networks. They're all potential targets.

Way to Stop This Type of Attack:

- Regularly update all systems and software to close known vulnerabilities.
- Use advanced monitoring tools like CrowdStrike Falcon to catch unauthorized access or unusual behavior.
- Implement IDS/IPS systems to monitor and block suspicious traffic in real time.
- Restrict user permissions based on the role only give access to what's absolutely necessary.

How to Prevent It in the Future:

- Schedule regular security assessments and penetration tests to identify weaknesses before attackers do.
- Adopt a zero-trust model, where every access attempt gets verified no matter where it's coming from.
- Train employees on phishing and social engineering since attackers often rely on these tactics to install backdoors.

Case 2: Facebook Account Hacking

The goal of This Technique:
The goal here is to exploit Facebook's account recovery system to take over an account. Attackers use recovery questions, phishing, or social engineering to impersonate the user. Once they're in, they can impersonate the victim, steal personal data, or use the account to scam others.

Who Would Be a Target?
Anyone with weak account security is a target, but hackers often go for high-value accounts like influencers or businesses. These accounts have more reach and value for spreading phishing scams or promoting malicious content.

Way to Stop This Type of Attack:

- Turn on Two-Factor Authentication (2FA) to add an extra layer of security.
- Use strong, unique recovery questions that aren't easy to guess.
- Keep your recovery contacts and emails updated and secure.

How to Prevent It in the Future:

- Facebook could improve by adding behavioral analytics during account recovery to flag unusual activity.
- Regularly review your trusted contacts and remove anyone you're not sure about.
- Educating users about phishing attempts and fake friend requests can help prevent these attacks from happening in the first place.

Case 3: Cookie Hijacking

The goal of Cookie Hijacking:
Cookie hijacking (also called session hijacking) happens when attackers steal session cookies, which store login data. With these cookies, attackers can impersonate the victim and access accounts without needing their password.

Who Would Be a Target?
The easiest targets are people on unsecured public Wi-Fi, like at coffee shops, airports, or hotels. Remote workers or travelers accessing sensitive accounts without additional security measures are also at risk.

Way to Stop This Type of Attack:

- Only connect to websites that use HTTPS, as it encrypts data and keeps it secure.
- Use a VPN on public Wi-Fi to add an extra layer of encryption and protect your data.
- Add browser extensions like HTTPS Everywhere to enforce secure connections.

How to Prevent It in the Future:

- Websites should implement HTTP Strict Transport Security (HSTS) to make sure all connections are encrypted.

- Avoid using public Wi-Fi for sensitive accounts unless you're connected to a VPN.
- Always log out of accounts when you're done, especially on shared or public devices, to invalidate session cookies.

Resources

- **Backdoor Attacks:**
    - What Is a Backdoor & How to Prevent Attacks in 2024 - SafetyDetectives
    - What are Backdoor Attacks? Types & Examples - SentinelOne
- **Facebook Account Hacking:**
    - 22 Tips to Protect Your Facebook Account from Hackers - wikiHow
    - Foolproof Steps to Help Protect Your Facebook Account from Hackers - CyberGuy
- **Cookie Hijacking:**
    - The Ultimate Guide to Session Hijacking aka Cookie Hijacking - The SSL Store
    - Cookie Hijacking - Invicti