Credential Theft & Identity-Based Attacks

ISE 331: FUNDAMENTALS OF COMPUTER SECURITY

TEAM 09 BUSHRA PARACHA | MOHAMMAD BAZAL | PANEET DHALIWAL

Shift in Cybersecurity

Traditional Attack

- Targets system or software weaknesses
- Attacker tries to “break in” from the outside
- Uses exploits, malware, or network vulnerabilities
- Security tools may detect unusual system behavior
- Main focus is protecting networks and devices

Identity Based Attack

- Targets user accounts and login credentials
- Attacker tries to “log in” as a trusted user
- Uses stolen passwords, tokens, cookies, or MFA approvals
- Activity may look normal because it comes from a real account
- Main focus is protecting identity and access

Sources: Verizon DBIR, 2024; NIST SP 800-63-3

Why These Attacks Are Effective

- These attacks target both technology and human behavior.
- Phishing tricks users into giving away login information.
- Password reuse allows one stolen password to affect multiple accounts.
- Stolen cookies or session tokens may let attackers bypass normal login steps.
- Because attackers use real accounts, their activity can be harder to detect.

Human Factor

- Phishing and social engineering trick users

Credential Weakness

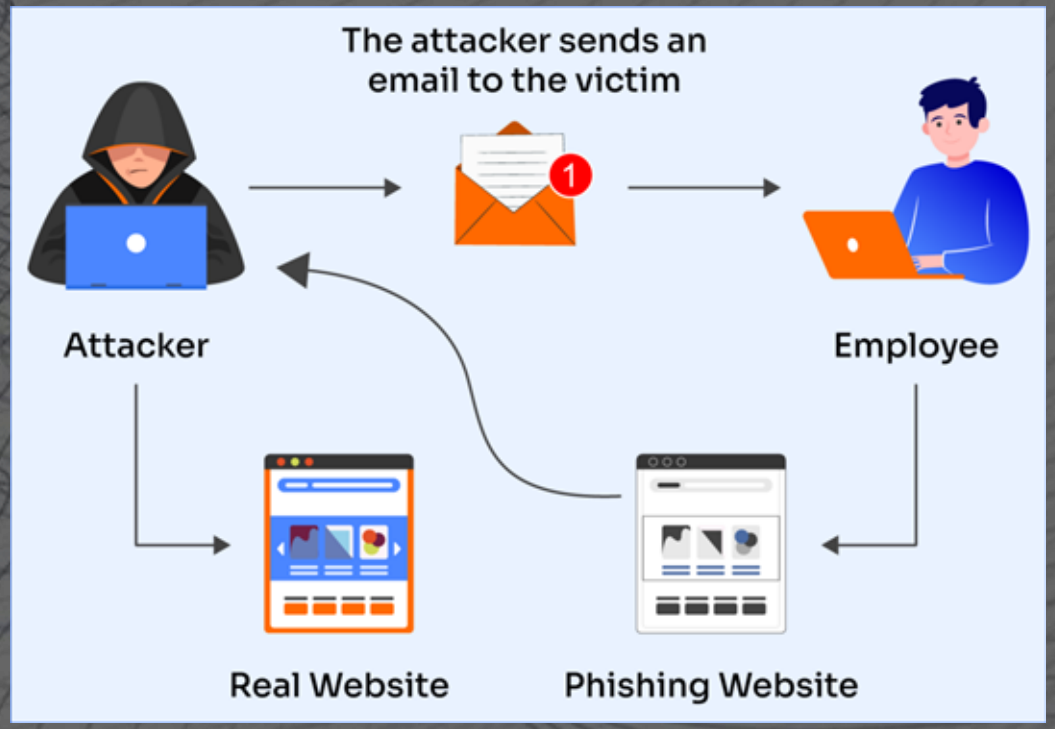
- Password reuse increase damage

Technical Bypass

- Tokens and sessions can avoid normal login checks

Sources: Verizon DBIR, 2024; OWASP, n.d.

Phishing Attacks



- Phishing uses fake messages, emails, or websites to trick users.
- Attackers often copy trusted brands, school systems, banks, or workplace login pages.
- The victim enters their username and password into a fake login page.
- The attacker collects the credentials and uses them to access the real account.
- Phishing works because it targets trust, urgency, and human error.

Sources: OWASP, n.d.; MITRE ATT&CK

Phishing Attack

Example:
A student gets an email:
“Your school account will be locked. Click here to verify.”

The email looks real:

- Same logo
- Same formatting
- Even a similar email address

The link goes to a fake login page that looks identical to the real one

Student enters username/password. In result the attacker now owns the account

From there, they can:

- Access your email
- Reset passwords for other accounts
- Impersonate you

Sources: OWASP, n.d.; MITRE ATT&CK

Phishing Attack Solution

Always check URLs carefully

- Attackers use slight variations like amaz0n.com

Avoid clicking links in emails

- Go directly to the official website instead

Enable Multi-Factor Authentication (MFA)

- Even if your password is stolen, attacker can’t login because they would need the second security metric in which you set up.

Think before reacting to urgency

- Real companies don’t pressure you instantly. Think carefully about what the email is talking about and remember especially if it's too good to be true.

Sources: OWASP, n.d.; MITRE ATT&CK

Password Reuse

- Password reuse means using the same password for multiple accounts.
- If one account is compromised, attackers may try the same password on other websites or systems.
- This technique is dangerous because one stolen password can lead to several account breaches.
- Reused passwords increase the impact of phishing, data breaches, and credentials stuffing attacks.

Sources: OWASP, n.d.; Verizon DBIR, 2024

Password Reuse Example

-You use the same password everywhere like on your chase banking account and lets say your playstation login lets say for example baz123@.

- If playstation has a network breach, the hackers will use the same email address and password on your chase account and have access.

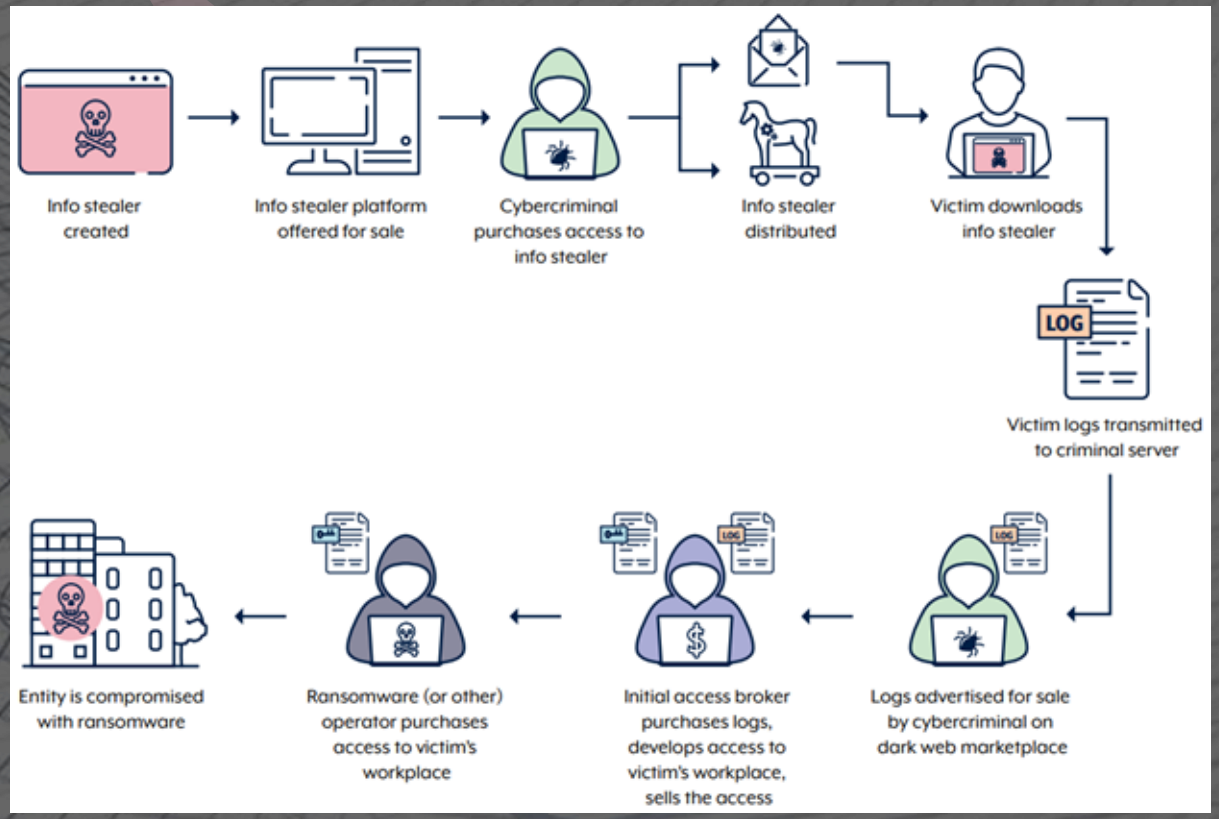
Sources: OWASP, n.d.; Verizon DBIR, 2024

Password Reuse Solution

- Using unique passwords and a password manager can reduce this risk .
- When you login to an app make sure that it is legit and not just a fake that collects information.
- Even if you do store all unique passwords somewhere do not store it in one place.

Sources: OWASP, n.d.; Verizon DBIR, 2024

Infostealer Malware



- Infostealer malware is malicious software designed to collect sensitive information from a device.
- It can steal saved browser passwords, cookies, session tokens, and other login data.
- This is dangerous because attackers may not need to trick the user after the malware is installed.
- Stolen cookies or tokens can sometimes help attackers access accounts without entering the password again.
- Infostealers make credential theft more automated and harder for users to notice.

Sources: MITRE ATT&CK; Verizon DBIR, 2024

Infostealer Malware Example

Let's say someone downloads a "free cracked version" of software or a game.

The file works—but hidden inside is an infostealer.

After installation:

- It scans Chrome/Firefox for saved passwords
- Collects session cookies (so attacker doesn't need your password)
- Grabs Discord, Gmail, or banking credentials

Within minutes, all that data is uploaded to the attacker.

Then:

- Your accounts get taken over
- Your email is used to reset other accounts
- Your identity is essentially compromised

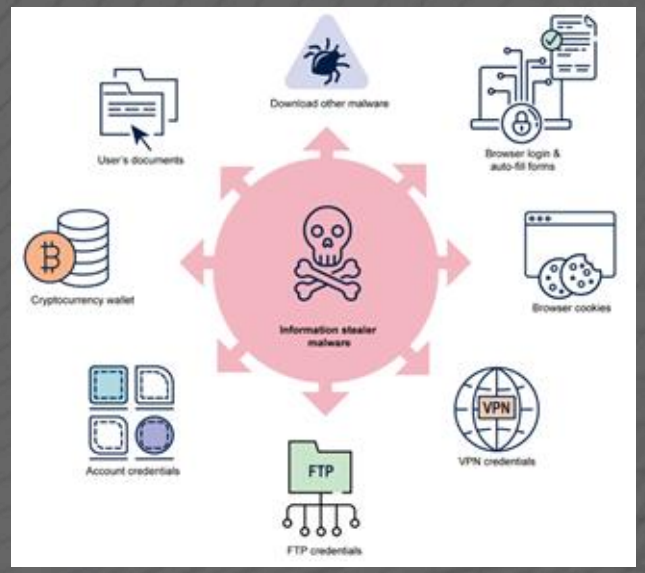
These stolen credentials are often:

- Sold on the dark web
- Used in credential stuffing attacks

Infostealer Malware Solution

Prevention

- Avoid downloading cracked/pirated software
  - This is the #1 source of infostealers
- Only install apps from trusted sources
- Use antivirus / endpoint protection
- Keep your system updated



Protection (If Compromised)

- Immediately change all passwords
- Enable MFA on all accounts
- Log out of all active sessions
- Clear browser data (cookies, saved passwords)
- Run a full malware scan or reset device

Smart Security Habits

- Don’t store important passwords in browsers
- Use a password manager instead
- Monitor unusual logins or account activity

Session Jacking:

Session hijacking happens when an attacker steals a user's session token, which is a small piece of data that proves you're already logged in.

When you log into a website:

- You don't re-enter your password every time
- Instead, your browser stores a session cookie/token

If an attacker gets this token, they can:

- Access your account
- Bypass login entirely

Session Jacking Example:

You're at a coffee shop using public WiFi.

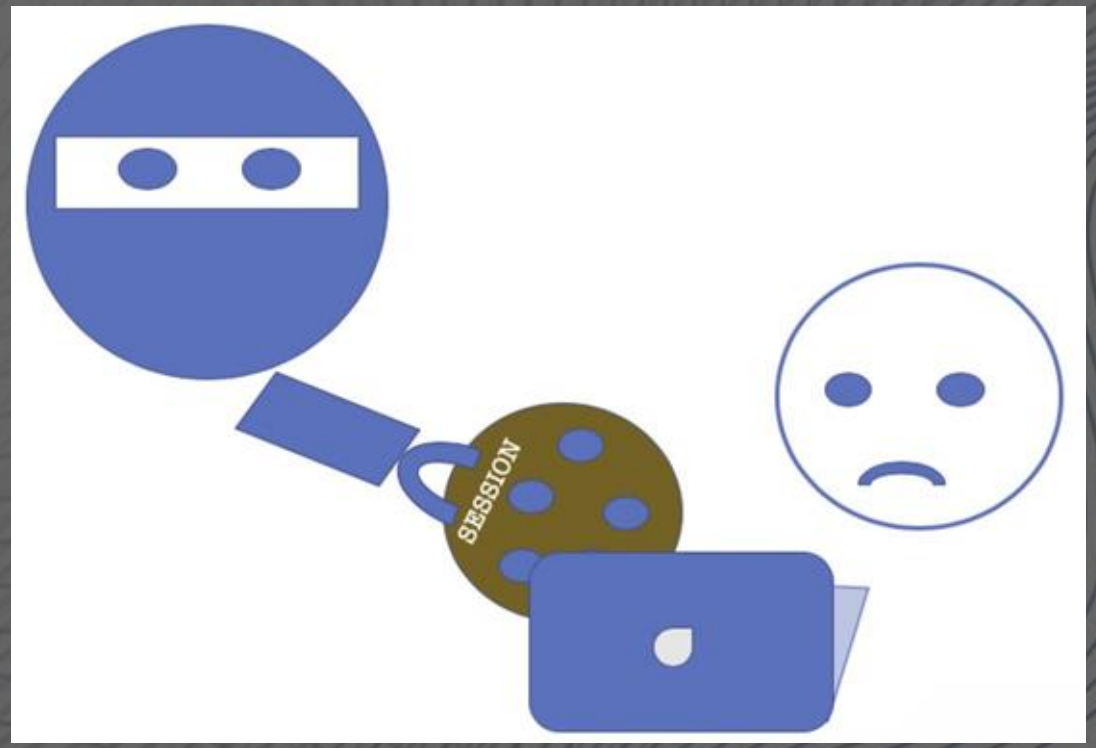
You log into your bank account.
Meanwhile, an attacker on the same network is running a tool that intercepts network traffic.

They capture your session token.

Now they:

- Open their own browser
- Inject your session token
- Instantly access your account

No password needed. No login alerts triggered.



Session Jacking Solution

- Avoid logging into sensitive accounts on public WiFi
- Use a VPN to encrypt your internet connection
- Only access websites that use HTTPS (look for the lock icon)
- Don’t stay logged in on public or unfamiliar computers
- Keep your browser and system updated for security patches
- Clear cookies and session data regularly
- Avoid clicking suspicious links that could steal session tokens
- Use secure, private networks whenever possible

Shoulder Surfing:

Shoulder surfing is a type of attack where someone physically watches you enter sensitive information, like passwords, PINs, or private messages, usually in public places.

Example:

Someone stands behind you in a coffee shop while you log into your bank

They watch your screen or keyboard

Now they know your password or PIN

Solutions

- Be aware of your surroundings when entering sensitive info
- Avoid typing passwords in crowded or public places
- Use a privacy screen protector on your device
- Shield your keyboard when typing passwords or PINs
- Sit or position yourself so others can’t see your screen
- Don’t leave devices unlocked or unattended
- Use biometric login (Face ID / fingerprint) when possible
- Lower screen brightness or angle it away in public
- Avoid accessing sensitive accounts in open environments

More Information(Learning Resources):

- Attend cybersecurity training sessions or workshops
- Take online courses on platforms like Coursera or Udemy
- Read cybersecurity books and academic articles
- Follow trusted tech blogs and security news sites
- Use official resources like National Institute of Standards and Technology (NIST)

More Information(Professional Help):

- Consult cybersecurity professionals or IT experts
- Work with security consulting firms
- Use company IT/security departments for guidance
- Participate in cybersecurity awareness programs
- Stay updated through organizations like Cybersecurity and Infrastructure Security Agency (CISA)

Summary:

- Phishing: tricks users into giving up credentials through fake emails/websites
- Credential Stuffing: uses leaked passwords to access multiple accounts
- Session Hijacking: steals active login sessions without needing passwords
- Infostealer Malware: silently collects all sensitive data from a device
- Shoulder Surfing: physically observes users entering private information

Best Solutions

- Use strong, unique passwords for every account
- Enable Multi-Factor Authentication (MFA)
- Avoid suspicious links, downloads, and public WiFi
- Stay aware of surroundings and online activity
- Use tools like VPNs and password managers

References

Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

OWASP Foundation. (n.d.). *Authentication Cheat Sheet*. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

MITRE. (n.d.). *Credential Access*. MITRE ATT&CK. https://attack.mitre.org/tactics/TA0006/

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital Identity Guidelines* (NIST Special Publication 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3