Account Hijacking: From Technical Breach to Digital Violence

Introduction

Account hijacking is far more than a technical problem—it often serves as a gateway to broader harm. When an attacker gains control of your account, they can access personal information, impersonate you to communicate with others, or exploit private content for blackmail. Many victims fail to recognize that hacking can constitute gender-based digital violence, yet its impact is equally severe: a loss of control and a persistent sense of threat.

Definition of Account Hijacking

Account hijacking refers to the unauthorized access and control of a digital account—such as email, social media, banking, or e-commerce accounts. Attackers may use the account to send messages, steal sensitive data, commit fraud, or engage in blackmail.

Potential Objectives:

- Financial theft
- Information gathering
- Identity theft
- Distribution of harmful or misleading content

Impact on the Victim

- Loss of personal data or reputational damage
- Harassment or blackmail carried out in the victim’s name
- Psychological distress, anxiety, and fear of engaging in digital spaces
- Violation of personal boundaries, leading to prolonged insecurity even after account recovery

---

Common Methods of Hijacking

- **Phishing:** Deceptive messages or links designed to steal login credentials
- **Password Reuse:** Exploiting stolen credentials across multiple platforms
- **Malware:** Software that records keystrokes or extracts files
- **Backup Email/Account Recovery Exploitation:** Taking over email or phone accounts to access others
- **SIM Swapping:** Transferring a phone number to a new SIM to intercept verification codes
  Social Engineering: Manipulating support staff or contacts to gain access
- **Third-Party App Vulnerabilities:** Granting permissions to untrusted applications

Signs Your Account May Be Compromised

- Unfamiliar activity or messages sent without your knowledge
- Password or associated email changes you did not initiate
- Login alerts from unknown devices or locations
- Loss of access to the account (rejected password, unknown recovery email)
- Repeated “reset password” emails you did not request
- Contacts receiving unusual links or messages from your account

Immediate Actions if You Suspect a Hack

1. Temporarily disconnect devices from the internet if malware is suspected
2. Document evidence (screenshots of login alerts, password changes, suspicious activity)
3. Attempt account recovery using platform recovery tools (backup email, recovery codes)
4. Change your password immediately for the compromised account and any accounts using the same password
5. Enable strong two-factor authentication (2FA) via authenticator app or security key; avoid SMS-based 2FA if possible

6. Scan devices with trusted anti-malware software or consult a technical expert
7. Log out of all active sessions from account settings
8. Report the breach to the platform, request removal of suspicious activity, and restore account access
9. Inform family, friends, or contacts if malicious content was sent from your account
10. Seek legal advice or contact cybercrime authorities if financial loss, blackmail, or threats occurred

---

Digital Safety Begins with Prevention

Account hijacking is not merely a technical glitch—it poses a serious threat to personal security and privacy. Employing strong, unique passwords, enabling two-factor authentication, and regularly monitoring account activity are proactive steps that prevent significant losses. Timely prevention and response protect your digital identity and help maintain control over your online presence.