🔐 Account Takeovers

Attackers get your password (or trick you into sharing a code) and lock you out of email, bank, or social accounts.

They pivot from one account to others using password resets.

🔗 Trusted Resources

FTC — Security & Password Tips — Strong passwords, passphrases, and 2FA guidance.

🌐 https://consumer.ftc.gov/articles/online-security ↗

IdentityTheft.gov — Federal recovery steps tailored to what was exposed. 🌐 https://www.identitytheft.gov/ ↗

Have I Been Pwned — Check if your email/passwords appeared in known breaches. 🌐 https://haveibeenpwned.com/ ↗

🧭 Recognizing & Responding Safely

Enable 2FA everywhere. Prefer app-based or hardware key over SMS where possible.

Unique passwords per account. Use a password manager.

If you get a login alert: Change the password immediately and review security logs/devices.

Account Takeovers

Locked out? Use the provider’s account-recovery process and remove any unfamiliar recovery email/phone on file.

Sam’s Tips

2FA stops most takeovers. Turn it on today.

One breach shouldn’t open every door. Unique passwords prevent chain reactions.

Recovery info is security too. Keep your backup email/phone current—and yours.