Introduction to Security

AP Cybersecurity · Vocabulary in context

Word	Example
Social engineering /ˈsəʊʃl ˌendʒɪˈnɪərɪŋ/	**Social engineering** tricks people into giving away secrets.
adversary /ˈædvəsəri/	An **adversary** is someone trying to attack the system.
elicitation /ɪˌlɪsɪˈteɪʃn/	**Elicitation** uses friendly chat to get secret information.
Intimidation /ɪnˌtɪmɪˈdeɪʃn/	**Intimidation** uses threats: “Do this now or lose your job!” “Do this now or lose your job!”
Urgency /ˈɜːdʒənsi/	**Urgency** makes people act fast without checking.
impact /ˈɪmpækt/	Smartphones have a big **impact** on how we learn.
challenge questions /ˈtʃælɪndʒ ˈkwestʃnz/	**Challenge questions** ask things like “What was your first pet’s name?” “What was your first pet’s name?”
impersonate /ɪmˈpɜːsəneɪt/	Attackers **impersonate** your bank to steal your password.
one-time password (OTP) /wʌn taɪm ˈpæswɜːd/	A **one-time password (OTP)** works only once.
malware /ˈmælweə/	A virus is a kind of **malware**.
password attack /ˈpæswɜːd əˈtæk/	A **password attack** tries to guess or steal your password.
weak /wiːk/	“123456” is a **weak** password. “123456”

Word	Example
dictionary /ˈdɪkʃənəri/	A **dictionary** stores pairs of keys and values.
authentication /ɔːˌθentɪˈkeɪʃn/	A password is a kind of **authentication**.
password manager /ˈpæswɜːd ˈmænɪdʒə/	A **password manager** stores all your passwords safely.
multifactor authentication (MFA) /ˌmʌltɪˈfæktə ɔːˌθentɪˈkeɪʃn/	**Multifactor authentication (MFA)** asks for a password and a code from your phone.
exploits /ˈeksplɔɪts/	Attackers use **exploits** to break into systems.
zero days /ˈzɪərəʊ deɪz/	**Zero days** are flaws that attackers use before a fix exists.
motivation /ˌməʊtɪˈveɪʃn/	Praise can raise workers' **motivation** to do good work.
Evil twin /ˈiːvl twɪn/	An **evil twin** is a fake Wi-Fi network with a real-looking name. Wi-Fi
access point /ˈækses pɔɪnt/	The Wi-Fi **access point** connects laptops to the network. Wi-Fi
SSID /ˌes es aɪ ˈdiː/	The **SSID** is the name of a Wi-Fi network. Wi-Fi
encrypted /enˈkrɪptɪd/	**Encrypted** data cannot be read without the key.
Jamming /ˈdʒæmɪŋ/	**Jamming** blocks Wi-Fi signals with noise. Wi-Fi
denial of service (DoS) /dɪˈnaɪəl ɒv ˈsɜːvɪs/	A **denial of service (DoS)** attack floods a website so no one can use it.

Word	Example
War driving /wɔː ˈdraɪvɪŋ/	**War driving** means driving around looking for open Wi-Fi. Wi-Fi
virtual private network (VPN) /ˈvɜːtʃuːəl ˈpraɪvət ˈnetwɜːk/	A **virtual private network (VPN)** protects your data on public Wi-Fi. Wi-Fi
deepfake /ˈdiːpfeɪk/	A **deepfake** video shows someone saying things they never said.
Large language models (LLMs) /lɑːdʒ ˈlæŋgwɪdʒ ˈmɒdlz/	**Large language models (LLMs)** write text, but they can make mistakes.
phishing /ˈfɪʃɪŋ/	A **phishing** email tries to make you click a bad link.
shared secret /ʃeəd ˈsiːkrɪt/	A **shared secret**, like a PIN, is known only to you and the bank. PIN
AI-enhanced coding tools /ˌeɪ ˈaɪ enˈhænst ˈkəʊdɪŋ tuːlz/	**AI-enhanced coding tools** suggest code that you must still check.
vulnerabilities /ˌvʌlnərəˈbɪlɪtiz/	Updates fix **vulnerabilities** in software.
threat detection and response /θret dɪˈtekʃn ænd rɪˈspɒns/	**Threat detection and response** spots attacks and stops them.
passphrase	A long **passphrase** of several random words is easy to remember and hard to guess.