LGBT TECH DIGITAL NAVIGATOR

ONLINE SAFETY PLANNING GLOSSARY

2-FACTOR AUTHENTICATION (2FA)

An extra layer of security that requires a second form of verification (like a code from your phone) in addition to your password.

ACCOUNT HIJACKING

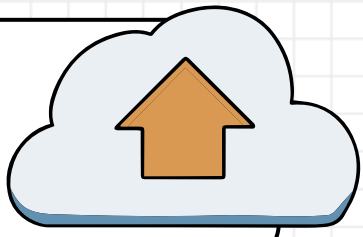
The unauthorized takeover of an online account by someone who gains access to the account owner's login credentials.

ANTI-MALWARE PROTECTION

Software tools designed to detect, prevent, and remove malicious software (malware) from computer systems.

BACKUP

A copy of your important data stored separately, so you can recover it if the original is lost or damaged.

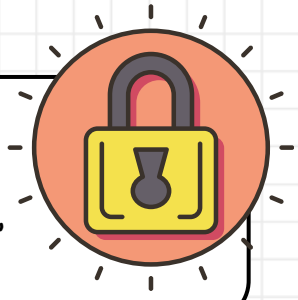


LGBT TECH DIGITAL NAVIGATOR

ONLINE SAFETY PLANNING GLOSSARY

CYBERSECURITY

The practice of protecting digital systems, networks, and data from unauthorized access, theft, damage, or disruption.



DATA BREACH

An incident where sensitive or confidential information is accessed, stolen, or used by an unauthorized person.

DATA CLASSIFICATION

The process of categorizing data based on its sensitivity and importance to the organization.

DOXXING

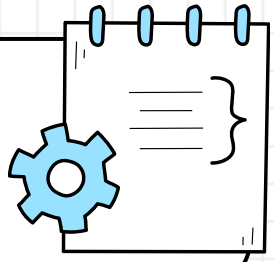
The act of researching and publishing private or identifying information about an individual or organization online, often with malicious intent.

LGBT TECH DIGITAL NAVIGATOR

ONLINE SAFETY PLANNING GLOSSARY

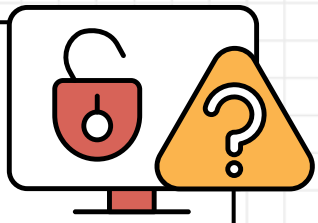
ENCRYPTION

The process of converting information or data into a code to prevent unauthorized access.



INCIDENT RESPONSE PLAN

A documented set of procedures for identifying, containing, and recovering from a cyber security incident.

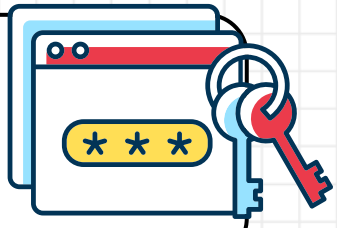


MULTI-FACTOR AUTHENTICATION

A security system that verifies a user's identity by requiring multiple credentials, such as a password, fingerprint, or security token.

PASSWORD MANAGER

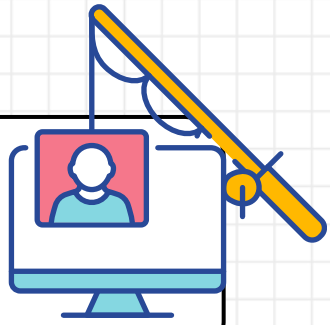
A secure software application that generates, stores, and organizes complex passwords for all your accounts.



ONLINE SAFETY PLANNING GLOSSARY

PHISHING

A type of online scam where attackers trick you into revealing sensitive information or installing malware, often by posing as a trustworthy entity.



RANSOMWARE

A type of malicious software that encrypts your files and demands a ransom payment to decrypt them.

SOCIAL ENGINEERING

Techniques used by attackers to manipulate people into revealing sensitive information or taking actions that compromise security.

VIRTUAL PRIVATE NETWORK (VPN)

A secure, encrypted connection between your device and the internet, which hides your online activity and location.