Cybersecurity

Policy Rationale

We recognize that the safety of our users includes the security of their personal information, accounts, profiles and other Meta entities they may manage, as well as our products and services more broadly. Attempts to gather sensitive personal information or engage in unauthorized access by deceptive or invasive methods are harmful to the authentic, open and safe atmosphere that we want to foster.

We do not allow:

Attempts to compromise or access accounts via unauthorized means, including:

- Accessing accounts, profiles, or other Meta entities other than one's own through deceptive means or without explicit permission from the account, profile, or entity owner.
- Obtaining, acquiring or requesting another user's login information, personal information, or other sensitive user information for the purpose of unauthorized access, including through the following tactics:
    - Phishing, defined as the practice of creating communications or websites that are designed to look like more trusted or reputable communications or websites for the purpose of fraudulently acquiring sensitive user information.
    - Social Engineering, such as repeated or consistent attempts to harvest or acquire the answers to common account or password recovery questions.
    - Malware, Greyware, Spyware or other malicious code, as described below.

Attempts to share, develop, host, or distribute malicious or harmful code, including:

Encouraging or deceiving users to download or run files, apps, or programs that will compromise a user's online or data security, including, but not limited to:

- Malware, defined as code or software designed to harm or gain unauthorized access to systems. This includes programs designed to harm computer systems, as well as software designed to extract money from victims, like ransomware.
- Spyware, defined as code or software that collects data on users and sends it to third parties without the informed consent of the user, or that uses the data for illicit purposes (e.g., sextortion, blackmail, illicit access to systems).
- Greyware, defined as code or software which detracts from the use of hardware or software and may be difficult to remove from a computer system or network.

- Creating, sharing or hosting malicious software including browser extensions and mobile applications, on or off the platform that put our users or products and services at risk.
- Threatening, admitting to, or enabling hacking - Including by sharing or advertising software, courses, or products that enable people to circumvent security systems, including software that encourages hacking of software or credentials
- Providing online infrastructure, including web hosting services, domain name system servers and ad networks that enables abusive links such that a majority of those links on our services violate the spam or cybersecurity sections of the Community Standards.