| Ransomware | Perform frequent backups of your system and other important files, and verify your backups regularly. If your computer becomes infected with ransomware, you can restore your system to its previous state using your backups. |
| --- | --- |
| Denial of service DDoS | Adding device-level and device-cloaking firewalling, external to the operating system, remains the most reliable form of DoS protection. Load balancing - Distributing traffic across multiple servers, a DoS attack can be prevented from overwhelming a single server or resource. |
| Spyware | Use trusted antivirus software with anti-spyware and anti-malware features |
| Malware | Always using a trusted antivirus program from a reputable provider. Running scans regularly. Always update your operating systems and software. Use security networks and proxies whenever possible. |
| Phishing | Configure user consent settings to allow users to only consent to applications that meet certain criteria |
| Worms | Use reliable antivirus software and firewalls |
| Data breaches | Enforcing strong credentials and multi-factor authentication to encourage better user cybersecurity practices |

Facebook cyber security breaches

Meta (formerly known as Facebook) has had numerous data breaches

Most of which were breaches of user data and privacy violations, beginning in 2007, and spanning all the way to present year 2023. In May 2018 a glitch prevented the privacy settings from working correctly. As a result, 14 million users’ private posts were shared publicly even though they were initially posted with viewing limitations. These posts became public without users’ knowledge or consent.

The bug was reportedly related to a new feature Facebook was testing, which rolled out on May 18, 2018. The bug was identified fairly quickly, but a fix for the problem didn’t begin rolling out until May 22, and the bug wasn’t fully resolved until May 27.