2021 Norton Cyber Safety Insights Report
How We Define Cybercrime

The definition of cybercrime continues to evolve as avenues open up that allow cybercriminals to target consumers in new ways. Each year, we will evaluate current cybercrime trends and update the report's methodology as needed, to ensure the Norton Cyber Safety Insights Report provides an accurate snapshot of the impact of cybercrime as it stands today. In the 2021 Norton Cyber Safety Insights Report, a cybercrime is defined as having personally experienced a crime committed with devices over the Internet. This includes crimes where a computer is used to victimize an individual, such as by theft or fraud, and crimes that target other computers and connected devices to access the data on the device or that affect the device's operation.

- Detected malicious software (e.g., spyware, ransomware, viruses, worms, Trojan horses, adware, etc.) on a computer, Wi-Fi network, smartphone, tablet, smart home, or other connected device
- Provided personal information, financial information or money in response to a fraudulent email, text message or website
- Learned your personal information was exposed in a data breach
- Discovered your personal information was stolen online and used without your permission
- Been threatened with the release of sensitive personal photos, video or information that was stolen online
- Detected unauthorized access to your home or personal Wi-Fi network
- Detected unauthorized access on a webcam
- Detected unauthorized access on a social media account
- Detected unauthorized access on an email account
- Detected unauthorized access on an online retail or shopping account
- Detected unauthorized access on an online banking or other financial account
- Detected unauthorized access on an online gaming account
- Detected unauthorized access on another online account
- Been stalked, bullied or harassed online