Scareware

Fear-based social engineering tactics are often used to trick users. It is often presented as legitimate software (antivirus, system cleaners, etc.) and uses fake alerts to scare victims into purchasing or installing useless or malicious software.

How does it work?

Pop-ups appear to “warn” that pornographic or dangerous files have been found on the device and will continue to appear until the buttons that “remove the threats” are clicked. They are designed to look like genuine warning messages, through the use of social engineering tactics. These tactics are designed to incite feelings of panic and fear. This is done to trick users into making hasty and irrational decisions and trick them.
The least harmful outcome would be losing money and installing useless software that does not fix the device, on the other hand, the most harmful option would be for the scammer to use the card numbers and personal data to steal money and commit identity theft. It could even take the contents of the hard drive hostage and a ransom may be required.
What cybercriminals want users to do is:

- Buy fake/useless software
- Download different types of malware.
- Visit websites that automatically download and install malware on devices.

Examples

Many scareware programs copy user interface elements from real malware protection programs and use legitimate-sounding names. Some examples are:

- XPAntivirus/AntivirusXP
- Antivirus360
- PC Protector
- Mac Defender
- DriveCleaner
- WinAntivirus