





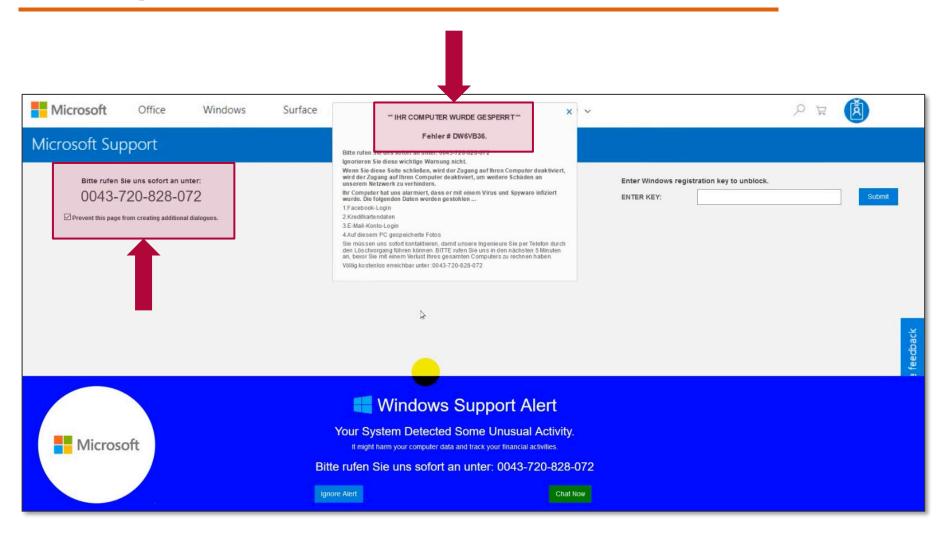
Scareware also called **rogueware** – malware (tactic) that scares users with the goal that they install malware to solve faked issues on their systems

- Uses social engineering attack method by showing fake messages, e.g., "virus detected", or "error message"
- Users then download or purchase software to solve these "problems"
- Is actually a malware that could steal personal user information or take control of user's system
- Often appears at malicious pop-up advertisements or spread via spam emails



Scareware and Rogueware **Example: Error # DW6VB36**





Scareware and Rogueware **Protective Measures**



- If possible, simply close the scareware
- Do not click any links displayed by the scareware
- Do not download or pay for any software suggested by the scareware
- Use Anti-Virus and Anti-Malware Programs to detect and remove the scareware