

Extortion

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

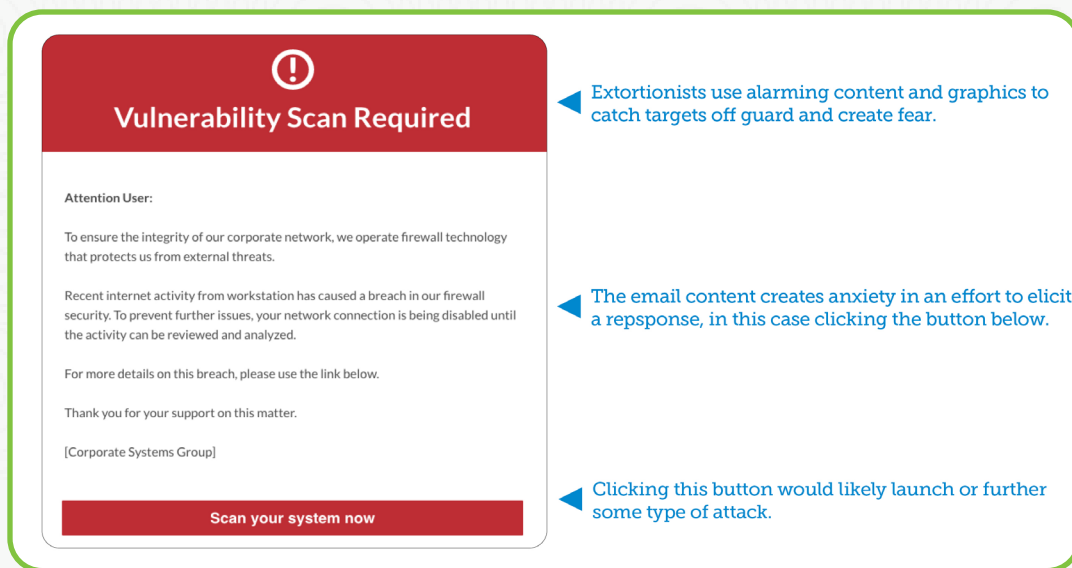
Extortion scams are increasing in frequency and becoming more sophisticated. In these types of attacks, cybercriminals leverage usernames and passwords stolen in data breaches, using the information to contact and try to trick victims into giving them money. The scammers may claim to have a compromising video or images from the victim's computer and threaten to share it with their contacts unless they pay up.

Extortion leverages a variety of emotions to elicit a response, including fear, shame and guilt. If you're targeted, you can prevent these types of cyberattacks from working by:

- Thinking rationally about the situation and keeping your emotions in check.
- Understanding that these types of attacks appear serious but are usually bluffs.
- Remembering that you are in control and that you have no obligation to respond.
- Reporting these emails to IT or the proper sources.

The sample shown highlights how extortionists craft their attacks.

Example



The example shows an email titled "Vulnerability Scan Required" with a red header and a warning icon. The body text is as follows:

Attention User:

To ensure the integrity of our corporate network, we operate firewall technology that protects us from external threats.

Recent internet activity from workstation has caused a breach in our firewall security. To prevent further issues, your network connection is being disabled until the activity can be reviewed and analyzed.

For more details on this breach, please use the link below.

Thank you for your support on this matter.

[Corporate Systems Group]

[Scan your system now](#)

Annotations on the right side of the email:

- ▶ Extortionists use alarming content and graphics to catch targets off guard and create fear.
- ▶ The email content creates anxiety in an effort to elicit a response, in this case clicking the button below.
- ▶ Clicking this button would likely launch or further some type of attack.