I

ILOVEYOU Worm: How the Love Letter outbreak spread

What it is ILOVEYOU, also called the Love Bug or Love Letter worm, was a major email-borne outbreak that began in May 2000. Its message used the subject ILOVEYOU and carried a Visual Basic Script attachment disguised as a text love...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

ILOVEYOU, also called the Love Bug or Love Letter worm, was a major email-borne outbreak that began in May 2000. Its message used the subject ILOVEYOU and carried a Visual Basic Script attachment disguised as a text love letter. Opening the attachment executed the worm on Windows systems.

How it works

The script overwrote or altered several file types, copied itself, changed Windows settings, and sent itself to contacts from the user's address book. Because the message appeared to come from someone familiar, recipients opened it quickly. Weak extension visibility and permissive scripting helped the outbreak spread at exceptional speed.

Key points

- ILOVEYOU is historically important because it combined simple social engineering with automated propagation.
- The original worm is old, but the same trust-in-a-contact tactic remains common in account takeover and phishing.
- A familiar sender does not prove an attachment was intentionally sent or is safe.

Lessons that still apply

- Show full file extensions and block unnecessary script attachments at the email gateway.
- Confirm unexpected files with the sender through a separate channel before opening them.
- Limit scripting where it is not required and keep reliable offline backups.
- Report suspicious messages quickly so administrators can remove copies from other inboxes.