Infocom
TRUSTED SECURITY

JE Infocom
8, Volodymyrska str.
Kyiv, 01001, Ukraine
tel.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

infoMail

Your Secure Communication

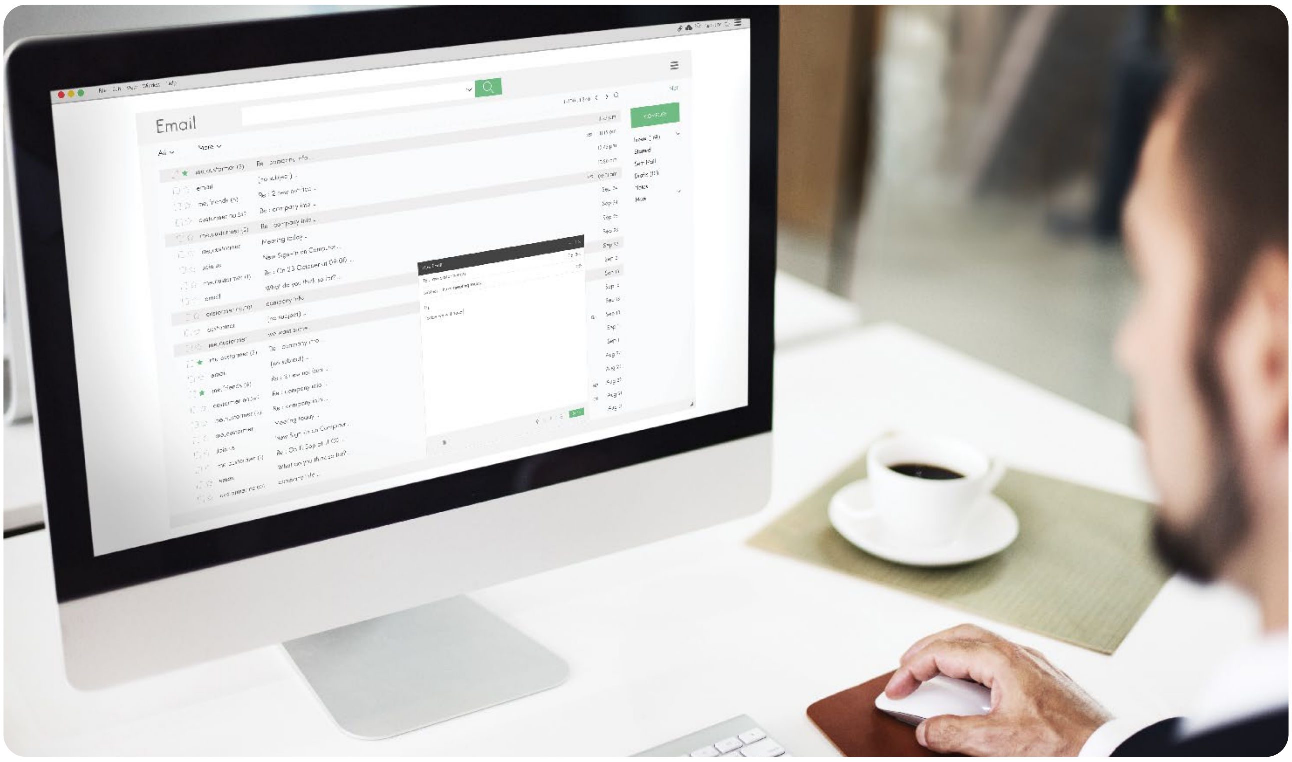
infocom.ua

2024

infoMail

Web Page

PROTECTION AGAINST EMAIL-BASED THREATS



Email remains the number one tool used by cybercriminals to achieve their goals, such as infecting users' computers, infiltrating networks, and stealing private or corporate information. Most of these attacks begin with "bait" or "reconnaissance" emails, which serve two purposes: to verify the existence of the victim's email account and to gather more information about the victim that cybercriminals can use for more targeted, combined attacks in the future. According to the Verizon 2022 Data Breach Investigations Report, 82% of successful attacks were executed by leveraging information obtained or access gained fraudulently to the user's computer or corporate network.

- The infoMail service is designed to combat modern, wide-ranging email-related threats such as viruses, malware, spam, emails containing links to malicious resources, data leaks caused by phishing technologies, and critical information leaks resulting from accidental or intentional unauthorized actions by employees. To effectively address these emerging threats, the analytics center of the equipment manufacturer hosting the infoMail service analyzes millions of emails globally per hour. It can identify new malicious codes within minutes and block all suspicious attachments found in emails for further analysis in cybersecurity labs.

- The most efficient and effective mechanism for protecting against spam and phishing messages is using reputation databases. When an email is received, the system checks the sender's IP address and content against such a database. If the sender has a negative reputation, the email is blocked.

infocom
TRUSTED SECURITY

Modern protection is unimaginable without reliable antivirus capabilities. The infoMail platform maintains a database with tens of thousands of virus signature variants across different malware families. Like the reputation database, the virus signature database is continuously updated in real time. During inspections, the antivirus analyzes attachment contents and, if necessary, unpacks archives, decrypts files, and removes active content from suspicious files and HTML attachments.

infoMail analyzes emails and sends suspicious files and links to a so-called cloud "sandbox" for further investigation. In the sandbox, a virtual environment is created where the suspicious code is executed as if it were in the recipient's real system. During this analysis, the system observes the suspicious code's actions, such as attempts to communicate with external servers for instructions or triggering processes that violate security policies. After the analysis, the system assigns an appropriate rating, which determines further actions, such as delivery approval or deletion.

Email protection can be implemented in two main modes: Transparent Mode or Gateway Mode.

- Transparent Mode

  Protection is implemented without changes to network or client software configurations. This is achieved by installing hardware and software directly on the mail server or client’s infrastructure, which handles email traffic.

- Gateway Mode

  Protection is implemented via hardware and software installed between the company’s internal network and the internet. All incoming and outgoing emails pass through this gateway for filtering and inspection.

infoMail Benefits:

- Reliable protection for your email and data
- Cost optimization by eliminating the need to purchase expensive equipment or licenses
- Reduced risk of business disruptions
- Time savings to focus on your strategic goals and tasks
- 24x7x365 support