



СП «Інфоком»
вул. Володимирська, 8
Київ, 01001, Україна
тел.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

infoMail

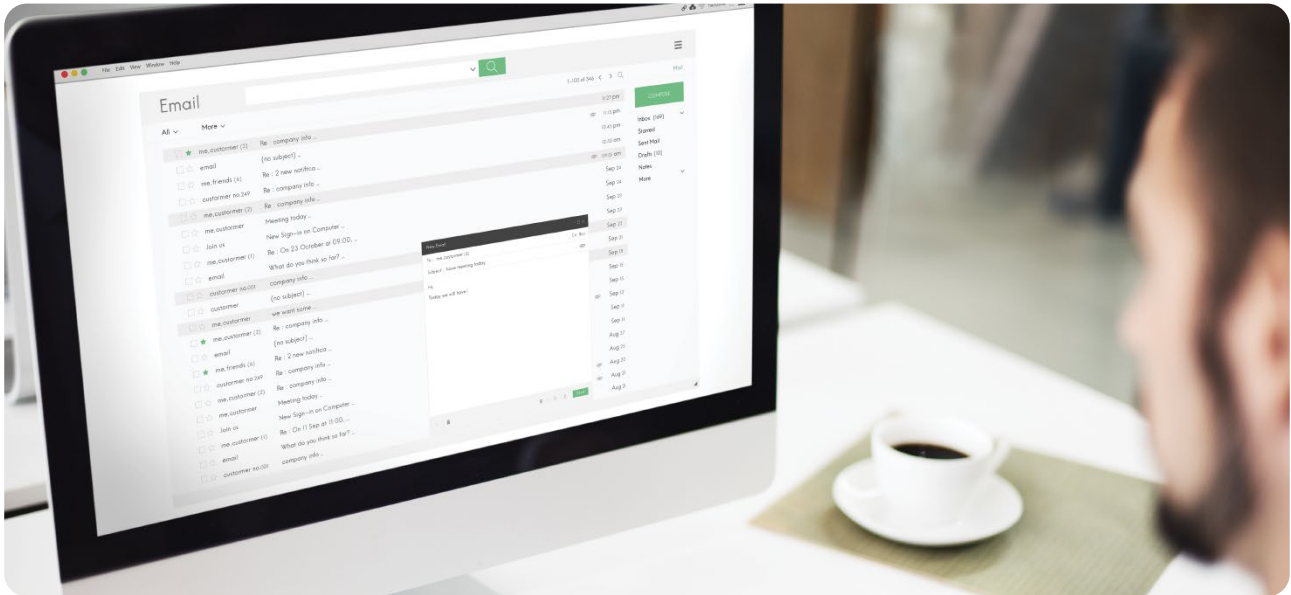
Захист електронної ПОШТИ



infocom.ua

2024

ЗАХИСТ ЕЛЕКТРОННОЇ ПОШТИ



Електронна пошта залишається інструментом номер один за допомогою якого кіберзлочинці досягають своїх цілей із зараження комп'ютерів користувачів, проникнення у мережі, викрадення приватної чи корпоративної інформації. Переважно, подібні атаки починаються з «приманки» або «розвідувальних» електронних листів, які служать двом цілям: вони перевіряють існування облікового запису електронної пошти жертви та намагаються зібрати більше інформації про жертву, яку кіберзлочинець може використати для здійснення цілеспрямованіших комбінованих атак у майбутньому. Згідно зі звітом VERIZON 2022 DATA BREACH INVESTIGATIONS REPORT 82% успішних атак було здійснено саме завдяки вдалому використанню отриманої інформації чи здобутому обманним шляхом доступу до комп'ютера користувача чи до корпоративної мережі.



Послуга infoMail розроблена для боротьби із сучасними загрозами широкого спектру, що виникають в наслідок використання електронної пошти такими як: віруси, шкідливе програмне забезпечення, спам, листи з посиланнями на ресурси, що містять шкідливе програмне забезпечення, витік конфіденційної інформації спричинений фішинг-технологіями, витік критичної інформації спричинений помилковими, або навмисними несанкціонованими діями працівників компанії. Щоб ефективно боротися з новими загрозами аналітичний центр виробника обладнання, на якому розгорнуто послугу infoMail, аналізує по всьому світу мільйони електронних листів на годину і може ідентифікувати новий небезпечний код за лічені хвилини та заблокувати усі підозрілі вкладення, виявлені в електронних листах для подальшого аналізу у лабораторіях інформаційної безпеки.



Найшвидшим та дієвим механізмом захисту від спаму та фішингових повідомлень є використання репутаційних баз даних. Під час отримання повідомлення на електронну пошту, система перевіряє IP-адресу відправника та вміст щодо наявності їх у такій базі. Якщо відповідний відправник має негативну репутацію, то лист блокується.



Сучасний захист не можливо уявити без надійного антивірусу. Платформа послуги infoMail налічує в своїй базі десятки тисяч сигнатур різних варіантів сімейств вірусів. Так само як і репутаційна база даних, база даних вірусних сигнатур постійно оновлюється у режимі реального часу. Під час перевірки антивірус аналізує вміст вкладень та, за потреби, проводить розпакування наявних архівів, розшифровує файли, видаляє активний вміст підозрілих файлів та HTML.



infoMail перевіряє електронні листи та надсилає підозрілі файли та посилання у так звану хмарну «пісочницю» для подальшого аналізу. У «пісочниці» створюється віртуальне середовище у якому підозрілий код запускається так, ніби він потрапив у реальну систему отримувача. Під час цієї перевірки аналізуються дії підозрілого коду, чи намагається він зв'язатися зі сторонніми серверами для отримання інструкцій, чи запускає будь-які процеси, які суперечать політиці безпеки, тощо. Після перевірки, система призначає відповідний рейтинг, згідно якому виконуються подальші дії, такі як дозвіл на доставку отримувачеві, або видалення.

Захист електронної пошти може бути реалізований у двох основних режимах: прозорому режимі та у режимі шлюзу:

- У прозорому режимі захист електронної пошти реалізується без змін в налаштуваннях мережі або клієнтських програм. Це досягається шляхом установки апаратно-програмного забезпечення безпосередньо на поштовий сервер або інфраструктуру клієнта, через яку проходить поштовий трафік.
- У режимі шлюзу захист електронної пошти здійснюється через апаратно-програмне забезпечення, яке встановлюється між внутрішньою мережею компанії та інтернетом. Усі вхідні та вихідні електронні листи проходять через цей шлюз для перевірки та фільтрації.

Послуга infoMail це:

- Надійний захист вашої електронної пошти та даних
- Оптимізація ваших витрат на забезпечення кіберзахисту завдяки відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього
- Зниження ризиків порушення діяльності вашої компанії
- Економія вашого часу та можливість повністю сконцентруватись на ваших стратегічних планах та задачах
- Підтримка 24x7x365