NEVERCLUELESS
Suite of Products

Encrypted Email

Encrypted Message allows your customers to send emails with end-to-end encryption – so important documents such as contracts or company plans can be safely and securely sent via email.

Why encrypt email?

Email is a convenient, fast and efficient way to communicate and share important information. However, it is an inherently insecure medium, as emails travels through multiple public and private networks and data lines between sender and recipient. Because email by default is sent in a unencrypted format, anyone who can intercept the email in transit, can easily access of its its contents, including any attachments.

By encrypting email with Encrypted Message, only the sender and recipients, who have a special decryption key, can read the contents of the message and its attachments. If someone intercepts an encrypted message, or tries to access it without permission and the decryption key, they will be unable to read the email or its attachment.

Who should encrypt email?

All businesses, and their professional advisors, agents and clients should take steps to protect the privacy of their email. Businesses that need encrypted email include:

Financial Services – Banks, brokerages, insurance companies, wealth management, accountants, financial advisors
Healthcare – Physicians, clinics, health associations, health networks, hospitals, pharmacists, pharmaceutical companies
Business Professionals – Lawyers, headhunters, investigators, consultants, human resource professionals, embassies

Businesses need to be able to trust email communications and reduce the risk of damage to their brand. Professional advisors such as lawyers, financial advisors, accountants, educators, and healthcare providers, all have ethical and fiduciary duties to keep their clients' personal information confidential.

Regulatory compliance controls risk and maximizes security

Governments have enacted legislative measures to protect the privacy and reliability of business and personal information. Encrypted Message meets these industry-specific privacy legislations including:

Health Insurance Portability and Accountability Act (HIPAA) is an example of legislation that protects personal information sent amongst health care professionals, such as patient health records, test results, x-rays, and prescriptions, are used, disclosed, and protected.

Sarbanes-Oxley Act (SOX) governs integrity of financial operations of publicly traded companies with the primary goal of protecting "investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws".

Gramm-Leach-Bliley Act (GLBA) required that all financial institutions (i.e., businesses engaged in banking, insuring, stocks and bonds, financial advice and investing) maintain safeguards to protect customer information.

California Security Breach Notification Act (SB 1386) required that companies, in the event of a breach of the security system of a database containing personal information (e.g. social security number; driver's license number of California Identification Card number; or account number, credit or debit card number, notify all California residents whose unencrypted personal information was in the database at the time of the data breach.

Fully managed email encryption solution

If your customer is already using your hosted Exchange service, then encrypting your mail is easy. With Encrypted Message, users can quickly, easily and intuitively send email with confidence. Encrypted Message is built on industry-trusted encryption standards, and provides the tools you need to simply and easily administer users. We host and manage the hardware and software needed to enable encryption and decryption processes, and management of digital identities. We administer the system and support you while you control your users.

How does it work?

The Encrypted Message solution includes a small desktop plug-in the works with Microsoft Outlook and Outlook Express. Customers compose their email messages, add any attachments, click the "Secure" button on the Encrypted Message plug-in toolbar, set their encryption password, and hit "send." It's that easy. When the recipients receive the message, Encrypted Message will prompt them for the password, and then decrypts the message. This simple process allows customers to quickly encrypt and decrypt messages without the hassle of managing a security and key infrastructure.

How Secure is it?

Encrypted Message uses standards-based technologies such as Public Key Infrastructure (PKI), S/MIME and X.509 certificates to enable the parties in a dialogue to establish confidentiality, message integrity and user authentication. This ensures the best commercially available encryption security for your messages.

What attachments does it support?

Encrypted Message can encrypt any MS Office document, .PDF file, image files, and almost any other popular file format.

How much does it cost?

Encrypted Message solution can be purchased on a per user basis. The solution is available per user per month, with a one-time setup fee per user.