BEYOND ENCRYPTION

Add-In Installation

OUR MISSION STATEMENT

To Secure You…

- Your Communication…
  - Your Data…
    - Your Identity

Contents

Introduction

Beyond Encryption is a secure email system designed to protect you and your customers from the unwanted attention of internet fraudsters intent on stealing your personal data.

Using simple software adapters, the system has been developed to integrate seamlessly with your current devices and email systems putting secure email just a single click away.

As a result of the trend in fraudulent IT activity, many businesses operate a strict 'lock-down' policy on devices and software and, as Beyond Encryption is best enjoyed using an installed adapter, it is important to articulate the ease with which they can be integrated into incumbent IT systems for both you and your customers.

This article defines the pre-requisites and installation process for an Add-In for the Microsoft Outlook email program, probably the most commonplace email program in use today.

What is an Add–In?

An Add-In is a software program that extends the capability of a primary software program; in this instance, the Beyond Encryption Add-In extends the Microsoft Outlook program to provide you with the ability to send and receive secure emails and to authenticate the identity of your intended recipient before you grant them access to the secure message content.

Why should I install it?

Read your secure email with a single click!

Although you will be able to read your secure email via your normal web browser, the Add-In allows you and your clients to open them in the same way that you open all of your other messages; directly from your Outlook Inbox.

Send secure email with a single click!

For security reasons, the send and reply functions may only be accessed when one of the Beyond Encryption adapters have been installed. The Beyond Encryption Add-In provides a 'reply' button when you read any of your secure emails and inserts a 'compose new secure email' button into your Outlook ribbon; these features allow you to reply and compose secure email directly from your existing Outlook email program.

Securing your data

When you send secure emails, your data is encrypted on your desktop by the Add-In before it is sent. Equally, any secure emails that you receive are decrypted on your desktop by the Add-In; your data is NEVER exposed on the internet as it is protected by our integral military grade encryption.

Build your own secure network…

When sending a secure email to a recipient for the first time, the Add-In prompts you to set a challenge to authenticate their identity before allowing them to open your email. Upon meeting your challenge, recipients are linked to your account allowing you to build your very own secure network.

Final check – should my email be sent securely?

With the Add-In installed, outgoing messages are checked for sensitive keywords such as 'confidential' or 'private'. Use this feature to ensure that you never send sensitive data in unsecured emails again.

What do I need?

The following pre-requisites are required to use Beyond Encryption with Microsoft Outlook.

- A computer capable of running Microsoft Office 2010.
- Microsoft Outlook 2010 onwards (both 32-bit and 64-bit options are supported)

Data Storage

When you sign up to use Beyond Encryption, we create a secure personal encryption vault into which we deposit your encrypted files when you send a message. This personal encryption vault is hosted within the EU on a secure Microsoft Azure platform.

If you wish, you may create your own personal encryption vault by connecting your own storage repository; the following repositories are supported:

- Beyond Encryption Data Store (default – no further data store configuration required)
- Dropbox
- OneDrive Business
- OneDrive Personal.

(Regardless of the storage option that you choose, Beyond Encryption are unable to access your secure information.)

For business users, integrations to your own 'on-premise' data storage facilities may be available; please contact Beyond Encryption for further details.

Using your own personal encryption vault allows you to take complete ownership and control of your data at all times.

Please note that where third party repositories such as Dropbox or One Drive are selected, you do NOT need to install any of their software; providing you hold an account and have access to the login credentials, Beyond Encryption will link the repository to your account and store your encrypted files for you.

Where can I get the Add-In?

The Add-In is available for download from our website www.besecuremail.com and is free to anyone that wishes to use Beyond Encryption to send or receive secure emails.

How do I install the Add-In?

You will require administrative permissions over your laptop allowing you to install a Microsoft Outlook Add-In. We encounter many instances where the installation of Add-Ins is controlled/managed by IT administration teams and we welcome the opportunity to work with these teams to support your installation.

When you download the Add-In from the website, it is packaged as an automated installer. During installation, your operating system and Microsoft Outlook program settings are detected and the correct version of the software for your system is installed; 32-bit and 64-bit variants of both your operating system and your Outlook programs are supported. A restart of Microsoft Outlook after the installation is all that is required to register the software.

Virtual/Remote Desktop scenarios

The Add-In installer deploys registry keys to the ‘Local Machine’ hive by default, making the Add-In available to all users of that machine.

When installing to virtual or remote desktop infrastructures, the Add-In may be downloaded from the website and installed to a server without deploying the registry keys that manage its behaviour; this may be achieved using the following command line:

```
BeOutlookAddin.exe /install BESETREGISTRY=0
```

Exposure of the Add-In to users may now be managed by adding the following mandatory registry keys to group policies etc:

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Outlook\Addins\Beyond Encryption]
"FriendlyName"="Beyond Encryption"
"Manifest"="file:///C:\\Program Files (x86)\\Beyond Encryption\\BEsecuremail.vsto|vstolocal"
"Description"="Beyond Encryption"
"LoadBehavior"=dword:00000003

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Outlook\Resiliency\DoNotDisableAddinList]
"Beyond Encryption"=dword:00000001

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\Resiliency\DoNotDisableAddinList]
"Beyond Encryption"=dword:00000001
```

There is an auto-update feature that IT administrators should also disable to allow them to manage the rollout of updates of the Add-In software.

Depending upon the architecture of the installed Microsoft Outlook version, key values go in the following registry hives:

For 32 bit:

```
    Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Beyond Encryption\Outlook Add-In
```

Or…

For 64 Bit:

```
    Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Beyond Encryption\Outlook Add-In
```

values are all strings:

```
      “UpdateNotifications_Enabled (false)”
```