Your public key is THE key to privacy

Imagine communicating via a medium that was easily intercepted, instantly filtered, that allowed anything exchanged between correspondence partners to be copied and made available to whatever 3rd party might be interested without you ever knowing.

Welcome to unsecured e-mail. It is used by hundreds of millions of users to generate billions of mails daily, many of which are sensitive in content and should not be made public. Users of unsecured e-mail asking for privacy display irrational behavior.

Why do people use unsecured e-mail?

That depends on the content of what we want to communicate and on the recipient. If what we send is sensitive material, or declared confidential, we better not use an unsecured medium. Should any dispute arise over the handling of confidential information, any court will consider an unsecured e-mail as a "deliberate voluntary disclosure of content by the sender". If what we send is publicly available information anyway, we may not care. But if we are concerned with maintaining confidentiality and privacy, if we do not want to disclose everything to unknown 3rd parties who may systematically capture and analyze not only whom we communicate with and when (=metadata), but what we say and send (content and attachments), we must act accordingly.

Why do e-mail users behave the way they do?

Most of us would prefer to have at least some level of certainty that our e-mail correspondence is read by the intended recipients only. At least most of the time.

Yet the majority of people use unsecured e-mail for communicating sensitive content. Apparently without the slightest doubt. As if privacy were none of their concern. Even those demanding privacy often behave as if it were somebody else's responsibility. Their problem. But not something they could easily address themselves.

Those of us who are digital natives and educated professionals must admit that we do know better. We are aware that unsecured e-mail is transmitted via the internet in a plain, legible format, stored and forwarded by multiple server and gateways, easily accessible to anyone who operates the systems. E-Mail is comparable to a postcard in many ways. Both can be read by anyone handling them. But e-mail is far more easily intercepted, filtered, investigated, copied, stored and forwarded than postcards; Because e-mail is digital. E-mail can be made available to whoever may have an interest in using the content for their own purpose, immediately and at practically no cost.

The potential for unintended use of information exchanged via unsecured e-mail is enormous. The cost of doing so is negligible. That’s a problem. Fortunately it can be resolved.

Why not secure e-mail using encryption?

Securing e-mail between a sender and a recipient by encrypting it is simple and costs very little. It requires the recipient to have a so-called secure e-mail certificate linked to the recipient’s e-mail address. The certificate needs to be installed once on the device(s) used for sending and receiving e-mail. In order for the sender to be able to transmit the e-mail securely, the sender needs access to the recipient’s public key. Not vice versa. That may not be obvious to e-mail users. They believe confidentiality is a sender's responsibility, whereas it is the recipient who enables secure communication.

Where's the problem?

Since it is the recipient's public key that is used, on the sender's device, to encrypt the content of e-mail sent to the recipient, it is the recipient's obligation to enable confidentiality and privacy for incoming e-mail. It is primarily the recipient, not the sender, who needs to have a secure e-mail certificate installed on their device.

Although having a secure e-mail certificate installed is strictly required it is not sufficient for a recipient to receive confidential information via encrypted mail.

Senders need access to our public key. In other words, we need to systematically ensure our public key is made public in the sense of easily accessible to any potential sender.

How do we make our public key public?

There are fundamentally three ways we can make our public key easily accessible to others, i.e. a wide range of potential senders:

(A) We can deliberately choose an identity provider for supplying our secure e-mail certificate who provides a publicly accessible search and download facility for public keys linked to e-mail addresses.

(B) We can deliberately choose to sign all our outgoing e-mail, which results in our public key being included in all mails we send.

(C) We can deliberately choose not to suppress the returning to the sender of digitally signed delivery confirmation receipts for digitally signed incoming mail.

All of these are highly recommended, preferably combined. Any one of them may enable a sender to send us, the recipient, encrypted mail.

Signing all outgoing e-mail is by far the easiest way of systematically giving recipients access to our public key. Any recipient of signed mail using any standard mail client on any standard e-mail capable device (notebook, tablet or smartphone) can then easily reply to the incoming signed e-mail and encrypt their outgoing reply. The only thing the recipient needs to be made aware of and capable of doing is finding and pushing the respective “encrypt” button in their mail client before sending the reply. It really is that simple.

What do recipients of encrypted mail need to be aware of?

Incoming mail that was encrypted with our public key cannot be decrypted by anyone unless they have access to our private key. Our private key is essentially a unique sequence of 0’s and 1’s, a very large prime number. This private key is usually uploaded into the operating system(s) of the device(s) we use for e-mail purposes and protected with a password of our choice. Access to our private key requires knowledge of the password. The private key is usually blocked after 3 failed attempts to access it.

A secure mail certificate serves to secure incoming mail only if the following holds true:

(1) Everyone (particularly the sender!) has access to our public key.

(2) No one except us, the legitimate owner of the certificate, has (the password used for protecting) access to our private key.

(3) The identity provider (IDP) we chose to supply our secure mail certificate is publicly accredited and (generally believed to be) trustworthy (i.e. commits to using verifiable, publicly disclosed cryptographic algorithms to generate unique key pairs). We are well advised to choose an IDP who operates a publicly accessible search and download service for public keys and resides in a country whose government we believe to honor their stated principles (i.e. not request IDPs to provide backdoors for use by government agencies).

As recipients we cannot force a sender to use encrypted mail when sending us sensitive content. As senders we cannot force a recipient to install a secure mail certificate and give us access to their public key.

If we do receive encrypted mail, we need to be careful opening attachments, unless the mail is signed by a sender we know and trust and the signature is valid. Encrypted mail, by definition, cannot be inspected at the mail gateways / servers of the mail providers for dangerous payloads. Incoming encrypted mail that is not signed should be treated with extreme caution (see article on “digital angels and demons” published on LinkedIn by this author).

What can we expect from others?

In a perfect world, digital natives interacting in a professional manner would always be in possession of - or easily obtain access to their respective public keys. All e-mail users, senders and recipients, would have their respective e-mail addresses secured by a digital certificate issued by a publicly accredited identity provider of their choice.

In any e-mail exchange, sender and recipient would have a secure e-mail certificate and easy access to their respective public keys. This mutual access to each other’s public keys would be automatic upon first interaction, before exchanging confidential information.

How does this work in practice?

Let's assume you both have a secure e-mail certificate that is linked to your e-mail address and installed on the device you use for sending and receiving mail.

Access to the recipients' public key is all that is required for the sender to be able to encrypt and thus secure outgoing mail, including any attachment, to the recipients. To do so the sender needs absolutely no additional information about the recipient's mail system. Neither sender nor recipient need to understand how encryption and decryption works. Nor do they need to make an extra effort to encrypt or decrypt.

Encryption of outgoing mail with the public key of the recipient is done instantly, on the device used by the sender, upon pressing the send button. Decryption of content and attachments with the recipients' private key is done instantly upon opening the encrypted mail. Encryption does not prevent

Similarly the recipient needs not worry about how the sender gets hold of the recipient's public key. The public key of the recipient is automatically returned to the sender via a digitally signed S/MIME receipt, generated by the recipient's mail client upon receiving a digitally signed mail from the sender.

One signed mail sent with a request for a signed return receipt is all the sender needs to get access to the recipient’s public key. Provided the recipient has a secure mail certificate from an accredited provider installed and does not suppress the automatic returning of signed receipts.

Maintaining confidentiality in communication via e-mail is simple. It requires some understanding and experience to set up multiple devices used for sending and receiving e-mail with a secure mail certificate. Configuration takes no more than 2-3 minutes per device used for a suitably qualified professional. Once the devices used are set up, encrypting outgoing e-mail is simple and decrypting incoming e-mail is fully automatic. Users need not understand cryptography to secure confidentiality and privacy.

Get yourself a secure mail certificate from a trusted identity provider, get someone to install it who knows what they’re doing and adhere to these simple rules:

- Always sign your outgoing mail, especially when encrypting. Digital angels always sign. They do no harm and reveal their true identity.
- Do not open attachments that come with encrypted, but unsigned mail. Only the devil encrypts without signing. For obvious reasons.

Encourage others to do the same.