Making E-mail Secure Is Just Not That Difficult

(NAPSA)—E-mail security is not the problem—it's how we use e-mail that is the problem. There has been no lack of press and attention regarding the insecurity of e-mail and the consequences of account hacking. Look no further than the latest elections, the Sony Pictures hack, the latest Yahoo compromise, etc. We hear about the problem all the time. What is missing from all the discussion is how to solve the problem.

E-mail in its stock form is inherently insecure but that does not mean that it must stay that way. With a little bit of effort, one can confidently send secure e-mail with virtually no risk of the contents being compromised.

An analogy is that of a car and a seat belt. Cars are useful and largely safe. But we can make them safer by buckling up. While seat belts were not used regularly for many years, today, we understand their benefit and they are widely used. We need to make e-mail safe and secure and we can do this when e-mail encryption becomes as widely used. So get ready to buckle up before sending.

E-mail Suffers From Two Problems:

The first problem is that the content of your e-mails is readable when the e-mail is "at rest" (stored on either your system or on the corporate or cloud-based server such as Gmail). E-mails that are at rest can be easily read by any administrator with rights to administer the system or by anyone with your e-mail address and password.

The second problem is guaranteeing your identity or the identity of someone sending you an e-mail. Your identity or that of any sender can easily be spoofed. You have no way to be confident that the e-mail you received was from who it claims to be, nor can anyone be confident that e-mail from you came from you. All one needs is a friendly e-mail server (i.e., one where you have administrator rights) to spoof e-mail "To:" and "From:" addresses.

While these problems are significant, there is a great and relatively easy way to buckle up when using e-mail that solves both problems.

Encrypting your e-mails end to end (E2E) from within the e-mail client solves the problem by ensuring that

Keeping e-mails secure can be simpler—and more necessary—than many people realize.

they are safe and secure at rest (and in flight). Your content might get hacked but the hackers wouldn't be able to read the content because it is encrypted. If your account has been compromised such that a third party has access, they wouldn't have access to your encryption keys and thus couldn't decrypt your content.

The second problem is solved with a technology that is closely related to encryption called Signing. When an e-mail is signed electronically, it guarantees that the sender is as advertised.

How does one get these protections? First, both sides of the communication need to agree to participate. It also takes an extra step, like buckling up your seat belt—you need to press a button (within your e-mail client) to secure your e-mail.

Modern encryption products such as those offered by Trustera let you encrypt and sign your e-mails using your existing e-mail accounts and using whatever platform you might like to consume and send e-mails. Trustera supports iPhone/iPad, Android, Mac, Windows, and Windows Outlook.

Much like with buckling up or backing up your data, we all know we should be more secure with our messaging and now we easily can. There is no better time than now to start encrypting your e-mails. It is just not that hard to make e-mail safe and secure. Though the hackers hope you don't….