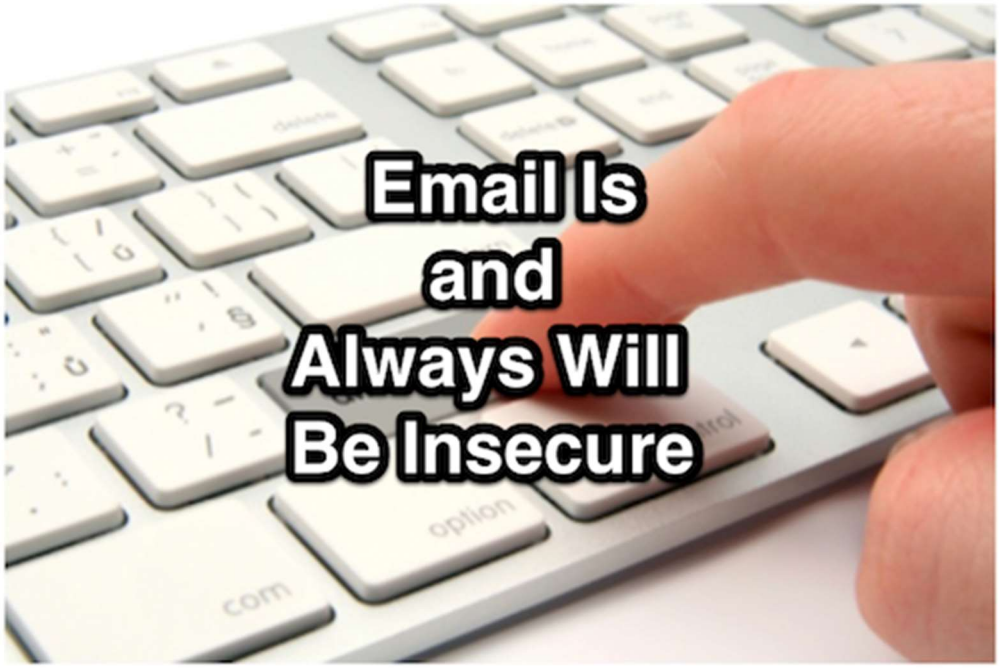
Email Is and Always Will Be Insecure



Email has been around for more than 30 years. One of the first and most useful functions of the web, email has allowed people to communicate quickly and efficiently regardless of location, time of day, and (more recently) language. Further, through the years, email has become linked with online identity, as web users employ their addresses to create accounts on websites and in stores, sign up for newsletters, marketing materials, and more.

Yet, despite email's endurance, flexibility, and continuing value, despite that there are more than 4 billion email addresses in use today, email remains one of the most insecure practices online – and that will likely always be the case. In initial stages, developers did not integrate any privacy or security into email, and though many efforts have been made to make email more sound, major obstacles prevent total protection of data. Users can and should make moves and develop habits to keep their emails (and the rest of their devices) safe, but by and large, email will never be truly secure.

The Trouble With Email

Email's initial developers never intended the service to become the integral web tool it is today. In fact, email was meant to be nothing more than the simplest way to send messages back and forth between different people on different devices. The messages were transferred in the open, meaning anyone with network or account access could intercept and read the transmissions. Today, that largely remains true.

A user's email messages can be compromised in four locations: the sender's device, the network, the server, and the recipient's device. The first and last should be comprehensible to anyone, regardless of tech savviness; email accounts are usually always logged in, so anyone sitting at a computer or holding a phone should be able to read any email message they choose. Email services rarely encrypt saved messages, so reading emails and attachments is as easy as opening the program or navigating to the webpage. Worse, most malware programs essentially do this – rifle through accessible emails for useful data – so this insecurity is more common than many users expect.

Networks and servers can provide differing amounts of security, based on senders' and recipients' email providers and internet connections. An email message might travel through dozens of routers and switches on its way to a recipient, and each transfer is an opportunity for cybercrime. There is no guarantee that each connection is equally secure; in fact, institutions like the NSA almost guarantee they are full of holes. Email servers are rarely encrypted – because of the overhead costs of encryption as well as the value of saving messages in plaintext (e.g., advertising) – so hackers with admin passwords or access through security flaws can search vast swaths of emails for personal data. From sending to receiving, saving to deleting, email is unbelievably insecure.

Making Email More Secure

Relying on email requires a large amount of trust: Users must trust their email clients, their networks, their servers, and their recipients to have sufficient security to keep their messages safe. Some of that trust can be ensured when users adopt third-party email security solutions. Because it is unlikely that email providers will spare the expense to protect email as thoroughly as they should, users must take personal action to bring email security into the 21st century.

Aside from malware scanning programs, email users' devices should be well-equipped with encryption tools. Encryption is by far the easiest and most effective way to prevent outsiders from reading messages they should not have access to. Users can employ public key cryptography, which encrypts messages and network connections, to allow private users to unlock sensitive data with secret passcodes. Within businesses, this system takes relatively little time to execute, but convincing everyone to adopt a public key encryption – everyone including clients, customers, family members, and friends – is somewhat unlikely. Thus, not all email messages can be secure at all times, even with an effective encryption system.

The Bottom Line

Email isn't likely to disappear in the coming years, even as other digital communications appear. Unfortunately, it is equally unlikely that email will become inherently more secure. Users must take it upon themselves to protect the emails they send – or else accept the likelihood of prying eyes on their private messages.

Author: Damian Davila

Ideas and concepts from Damian Davila, Ecuatoriano thriving in Hawaii. Pro marketer and blogger. Find him at @idaconcpts on Twitter. View all posts by Damian Davila