- AUTHOR: JOHN ACKERLY, VIRTRU.JOHN ACKERLY, VIRTRU

INSECURE EMAIL IS HERE TO STAY: LET'S FIX IT

In his thoughtful parsing of what email is and will become in The Atlantic, Alexis Madrigal writes that email is the "exciting landscape of freedom amidst the walled gardens of social networking and messaging services." Email is easy, open, and ubiquitous. We spend as much as 80% of our workday in our email inbox and use email for important personal communication. The Radicati Group reported in 2012 that 144.8 billion emails are sent every single day. That's 38 trillion emails a year. Email is here to stay.

Few would consider email to be a new technology. It's been around for more than 30 years, but remember that it only started to take off in the 1990s alongside the Web. Most people started using it 20 years ago, and in three decades email hasn't had much of an upgrade, especially when it comes to security.

Every email we send is insecure by default. While Google and Yahoo have taken positive steps to encrypt traffic, the basic protocols are still all plaintext, and forget about controlling the emails you compose after you hit send. While an email address routes your message to a recipient, there's no ability to recall or encrypt messages baked into this 30-year-old standard.

Email is here to stay, but what's also here to stay is the steady stream of gaffes and scandals created by the lack of security and control. Email is insecure by design. From Snowden's leaks to Wikileaks, to every scandal that hits the newswire, all of these stories are rooted in email's weak approach to securing information.

Case in point: just a few weeks ago Goldman Sachs mistakenly sent a sensitive email with account information to a random Gmail user because someone fumbled some keystrokes and sent to a "gmail.com" account instead of a "gs.com" account. The email contained such sensitive information that the only recourse Goldman had was to get a court order to require Google to retract the message.

Just this month, the UK's Information Commissioner "sounded the alarm" for lawyers in an attempt to get them to realize that unencrypted email is an unacceptable risk for privacy.

Recipe for Viral Success: The Embarrassing, Inadvertent Email

On a personal level, everyone who uses email understands the blunders and glitches that lead to sending an inappropriate email to the wrong recipient. Everyone understands what happens when people forward embarrassing emails to a larger group. While some have retreated to messaging apps that only allow messages to live for 10 seconds like Snapchat, most are still relying on email for both personal and professional communication.

Sending an unencrypted email with secret or embarrassing information in 2014 is not unlike placing a sensitive phone call to a small town in 1956 served by a shared "party" line that was typical for rural telephone service in the last century. Then as now, the potential for eavesdropping and for privacy violations is very much the same. The difference is that email blunders in 2014 are much, much riskier than a party line call was in 1956. An overheard phone call could lead to embarrassment or hurt feelings — an intercepted email can go viral.

From the Deranged Sorority Rant to a product rant from Bill Gates to Oxford University mistakenly emailing a list of the 50 worst performing students, this list could be extended to fill an entire page with illustrations of email's inherent lack of security. Some of these incidents are famous, but most are not. The common theme is that they never needed to happen. If everyone agreed to start using sensible tools built atop standard email to give senders and recipients some semblance of control, these gaffes would be a thing of the past. Sure, we'd have less entertaining email scandals, but we'd all be more secure in the end.

Moving Beyond Trust, Securing Email

When you send an email, that email is plaintext and stored on someone's servers. You are trusting the IT administrators at your company or your provider to not read through your email. When you send a highly personal email to a friend or loved one that contains information you wouldn't want shared with the world, there's absolutely no guarantee that your message is protected in transit or at rest — and, worse, there's no ability to take back an embarrassing email sent to a recipient if something changes.

We need to use technology that can enforce access control and encrypt. When you send a message it should be cryptographically signed and verified as a matter of course. We need to make the idea of sending unencrypted emails that can't be revoked or controlled seem as antiquated as an old telephone party line, and we have the technology to do this. Email needs an upgrade. Insecure standards need to be retired, and security and privacy need to be a priority. Whether you are motivated to act because of the security of your business or family, or you want to help put an end to government overreach and mass surveillance, it's time to put our party line email system away and start encrypting end-to-end today.

John Ackerly is co-founder and CEO of the digital privacy company Virtru.