



Email Encryption: 10 Things You Don't Know that Can Hurt You

The fact that email allows two people on totally separate networks to communicate across thousands of miles is one of its undeniable benefits, yet this incredible flexibility is also one of the reasons that data transmission via email is so challenging to conduct securely.

Email Encryption: 10 Things You Don't Know that Can Hurt You

Despite the fact that nearly everyone uses email constantly to exchange information, email is an inherently unsafe system. The fact that email allows two people on totally separate networks to communicate across thousands of miles is one of its undeniable benefits, yet this incredible flexibility is also one of the reasons that data transmission via email is so challenging to conduct securely.

Data security needs to be at the forefront of every company's mind, especially considering the literal terabytes of information exchanged on a daily basis during a standard business day. Information is shared among individuals, within companies and between organizations, yet rarely is security included as any consideration in daily practice. Sending an email has become so commonplace that the idea of added protection has simply fallen off the radar. In an effort to emphasize how much security matters even when sending an email, there are 10 things about email you never knew that could cause problems for you or your business.

In reality, SSL can only protect the sender's email on its first step: the quick trip between leaving your computer and arriving at your home email server. This lack of protection makes it easy for hackers to sniff emails in transit.

1. Emails Can Be Sniffed in Transit

By default, emails are typically sent without any form of encryption to protect them in transit. This means that anyone with the skills, knowledge or free time to read the content of that email could easily access it—not just once, but at several points throughout its journey. As emails travel from the sender to the recipient, they travel through multiple servers along the way. This means they're stored in many locations at different times: the sender's email server, servers en route, and the recipient's email server. Any one of these servers has the capacity to intercept that message and its contents.

SSL- or TLS-encrypted emails are purported to add another layer of security to this process. In reality, SSL can only protect the sender's email on its first step: the quick trip between leaving your computer and arriving at your home email server. This lack of protection makes it easy for hackers to sniff emails in transit. The physical server disks can also be sniffed for data via backup tapes or after being decommissioned.

2. Senders and Recipients Can Be Altered

It's advice that goes back to the days when AOL was all the rage: Don't open anything that isn't from someone you know. Yet, it's incredibly easy to fake or alter either sender or recipient on an email for even an entry-level hacker. It's also easy to reroute emails to a completely different destination by altering the DNS.

The default SMTP email protocol doesn't require any verification that the person listed as the sender of an email is in fact the actual author. Virtually anyone in the world could grab your email address and stick it in the "from" box, and only a handful of people would ever know the difference. Even when emails seem to be from known and trusted individuals, the only way to truly verify that is with an extra precaution, such as including a digital signature.

3. Viruses Can Affect Emails

The vast majority of email users know by now that any email attachments should be left right where they are until after passing a virus scan to make sure they're clean. However, very few of these computer users realize that there are more ways to transmit a virus than through a simple attachment. Not every virus crashes a computer either; some just lie in wait until the right moment, quietly gathering data in the background. As an example, there are viruses that scan emails as they arrive on an infected computer. These little sniffers can collect all kinds of sensitive data like passwords, account numbers and more, often without any other active symptoms to let you know you're actually under attack.



4. Senders Have No Clue What Recipients Are Doing

Email is essentially an entirely trust-based system. The sender trusts that the recipient is legit, and the recipient believes the same. Yet, even when both parties are entirely free of any malicious intent, email communication can leave both parties vulnerable.

Any email is out of your control the instant you hit send. After that, one of several things could happen:

- The recipient could forward the email to unauthorized parties, with or without your knowledge.
- The recipient may leave the message sitting unopened in his or her inbox, making it vulnerable to hackers.
- If the recipient's account is compromised, then the sender's data ends up compromised as well, regardless of how many other precautions have already been taken on the sender's end.

No matter how many steps have been taken to safeguard email and servers from the sender end, the integrity of the servers at the recipient end (as well as the actions of the recipient) are beyond the sender's control. Even sensitive documents that ought to have limited lifespans may not be archived or deleted according to regulatory guidelines, but there's simply no way to be sure.

The majority of email servers don't bother with regular backups; that's the end user's responsibility. In the event of an email client crash, all those archived attachments could be lost permanently.

5. Emails Aren't Automatically Backed Up

Emails are used for much more than casual conversations. Legally binding contracts, financial paperwork and even HR documentation may be (and often is) sent via email. In the old days of hard copies, all these vital forms would be copied and filed—probably in multiple places, just to stay on the safe side.

Because so many email services are now cloud-based, it's easy to assume that some type of automated backup system is already in place for anything important that arrives via email. On the contrary, the majority of email service providers don't bother with regular backups; that's the end user's responsibility. In the event of an email client crash, all those archived attachments could be lost permanently.

Whether setting up a cloud-based system for backup like Dropbox, storing documentation on a hard drive or exporting data to a removable storage device, committing to some type of backup protocol is essential for any email user.

Using a personal email address bypasses all of these protective measures; sensitive data transmitted through standard channels rather than secure ones is at far greater risk for a breach of some kind.

6. Using Personal Addresses for Corporate Emails Isn't Secure

While the majority of businesses today have their own dedicated email host and domain, that doesn't mean that all employees are actually using the service. This may be because they're attached to a particular personal email address, or because they feel that the functionality of their existing email provider is easier to navigate. Whatever the reason, a personal email address should never be used for transmitting business communication.

Organizations typically invest a great deal of time and money into ensuring a safe, secure internal network, often including encrypted wireless connections, encrypted email functionality and other security protocols. Using a personal email address bypasses all of these protective measures; sensitive data transmitted through standard channels rather than secure ones is at far greater risk for a breach of some kind. Some employees may put the entire company at risk by continuing to use personal email, as this act may constitute a violation of industry-specific guidelines such as HIPAA.

In email systems that have an automated backup protocol, all communications may be backed up on a remote server somewhere without your direct knowledge.

7. Deleted Emails Aren't Really Deleted

After receiving (or sending) an item that isn't work-appropriate, the normal reaction is to immediately delete it to stay on the safe side. The bad news is, even if both the sender and the recipient delete an email, it's not necessarily gone forever. In email systems that have an automated backup protocol, all communications may be backed up on a remote server somewhere without your direct knowledge. If needed for any reason—for example, in case of litigation—a skilled digital forensics professional can track down deleted emails and restore them.

Digital data may seem ephemeral but in some ways it's almost more permanent than physical documentation, because it so often seems gone when it really isn't. This is a good thing to keep in mind, particularly when sending or receiving emails in a work environment.

8. A Logo Doesn't Equal Security

It used to be that phishing emails were easily spotted as obvious fakes. These days, spotting a forgery in an inbox can be a real challenge. One way that companies show their communications are authentic is by including something recognizable, like using a particular color scheme or including their logo. Yet, even these are not necessarily indicators that an email is really from that sender.

Picture this: In a room full of cabinets that are sitting wide open, there is a single cabinet that's closed and locked. Which one is most likely to attract the efforts of a thief?

As hackers grow more talented and motivated, recognizing legitimate email communications becomes more difficult. The best way to prevent problems is to assume that any company that asks for a password, account number or other sensitive information is faking it. Instead of looking for a logo, get on the phone and obtain verbal verification of the message's contents if further clarification is needed.

9. Encrypting Single Messages Does More Harm than Good


Those users who are aware of the inherent risks present in sending and receiving emails are often also savvy enough to encrypt those specific messages that do contain any data that needs extra protection. While it's true that encrypted email service does provide an excellent additional layer of security, only encrypting a few emails here or there is a terrible idea.

Picture this: In a room full of cabinets that are sitting wide open, there is a single cabinet that's closed and locked. Which one is most likely to attract the efforts of a thief? Similarly, a lone encrypted email amid hundreds of non-encrypted ones is bound to attract the worst kind of attention from any hacker who's worth his salt. Make the commitment to either encrypt all emails full-time, or choose another communication method for information that needs to be more secure.

The truth is, no matter how much effort either the sender or the recipient puts forth to protect themselves, each other and their communications, it's possible that emails can be tracked, traced and opened without much effort.

10. Email Isn't as Safe as You Think

By now, it should be clear that the most important thing that can hurt email users is trusting in email's implicit safety. The truth is, no matter how much effort either the sender or the recipient puts forth to protect themselves, each other and their communications, it's possible that emails can be tracked, traced and opened without much effort. This is one reason that truly critical business or personal information should never be sent over email; use a more secure approach instead. Or, if emails must be used, at least encrypt all data that's sent or received so that any intercepted messages can't be so easily accessed.



If you would like to learn more about
how iBridge can help you with
your email encryption,
please contact us.

info@ibridgellc.com
503.906.3930

Follow us!

