Data Protection

Our personal information has never been so easy to steal. And mostly we have ourselves to blame.

Come again? Companies and consumers have been warned against sending out sensitive information as email attachments. And yet many companies still send out credit card forms and signature details. Medical offices use email for their patient communication. People accept and return emails with attachments that contain everything from their financial balances to their medical history. After all, the message is directed only to the recipient, so what can go wrong?

Emails are particularly vulnerable to cyber theft because they are stored in a variety of places, including, of course, the sender's and receiver's device. If someone hacks into your computer, your email is just sitting there for them to read. Rifling through email is now the most common process of malware, and malware is everywhere. The other points of possible attack are your Internet Service Provider and the sender's or recipient's. If your email is hosted on a service provider like Gmail, then it, too, is subject to attack. There are network connections between these email providers. How could you possibly know if all those connections are secure?

And that's not the only places where a copy of your email might be stored. Each email service provider keeps messages in archive on its own servers, which can be hacked and messages downloaded by cyberthieves. The bottom line: once an email message leaves your server, or leaves the sender's server, it's out of your control.

What can you do? The first and simplest rule of cyber safety is never to send sensitive information in an email message or an attachment. That means avoid including Social Security numbers, passwords, sensitive tax or investment account information, and even date of birth in your messages, even to people you trust. If you must communicate this type of information, there are a variety of much safer ways to share information, including ShareFile, PeerLink, Box, FileCloud and DropBox. Or you could encrypt your email messages using programs like Infoencrypt or SafeGmail. The messages are encrypted at the sender's computer and decrypted within the recipient's browser, and they

remain encrypted in both the sender's and receiver's email boxes. Hackers who gain access to your computer, to the service providers or the archives come away with nothing but unreadable gibberish.

Yes, protecting yourself sounds like a hassle. But all of these programs, and others, are much more user-friendly than they were ten years ago. And being careful with your messages is a lot less time and trouble than dealing with a stolen identity or having your personal information floating around the Dark Web.

Sources:

https://financesonline.com/top-10-file-sharing-services

https://digitalguardian.com/blog/what-email-encryption

https://www.howtogeek.com/135638/the-best-free-ways-to-send-encrypted-email-and-secure-messages/

https://www.linkedin.com/pulse/why-its-ok-send-sensitive-information-over-email-christina-harbridge/

By Bob Veres, publisher of Inside Information - the premier publication of financial industry trends and information for leading practitioners in the financial planning profession.