I'm John Sturtevant, and this is Say What?! A weekly podcast with quick tips to help you communicate clearly at work, at home, and everywhere else you go.

Welcome to Say What?! Episode 12.

This week, we continue our series: Ten Quick Tips for Terrific Email

And today's Quick Tip is: Let's make this a private conversation.

The other day I was taking my morning walk and thinking about ideas for this week's podcast.

As I turned a corner, I noticed a sign posted in front of a house. It read: This is a private sign, please do not read it.

Well, of course I laughed. But as I walked on, I thought hmmm actually, that's a lot like email.

We send people messages we think are private. But those emails are about as private as that sign was.

And many people add disclaimers to their email stating if you receive it in error, please do not read it, and destroy it immediately.

Well, as attorney Marc Reiner said in a recent Wall Street Journal article - that disclaimer has about as much legal influence as a mattress tag.

Everything we send in an email could end up on Facebook, Instagram, Tumblr, Tic Toc, and Twitter.

Your messages can be intercepted and read anywhere along the path between you, the sender, and your reader, the recipient.

And, your emails can even be reconstructed and read from backup devices long after you've deleted them, and forgotten them.

If you're sending email at work, your organization can legally monitor it, and if your company becomes involved in a lawsuit, parties involved have the right to review all employee email.

Your company probably asked you to sign an email policy, which described how email is to be used only for business purposes, and that the computer systems are the property of your employer.

Basically, you signed a contract agreeing none of your email is private.

Even if there is no signed agreement, an employer can still peek into your email, or your desk for that matter.

And if you send email in connection with public business, it is a public record even if was written and stored on your private computer.

If you send email from home, hackers can intercept it in multiple ways along its journey. Even your Internet service provider may legally be able to scrutinize your email.

According to LinkedIn's recent Cybersecurity Trends Report, employees are far more likely to exchange sensitive files directly from their office or home computers rather than using a cloud-based service.

And while cloud-based services are generally more secure than your laptop, everything can be, and is, hacked by bad people who spend their nights creating new ways to break into stuff.

Email encryption technology is available, but it's cumbersome to use and adds a layer of complexity to an otherwise very simple process.

One reason email is so popular is that it works so easily. It's trusted, but generally not secure.

In fact email was never meant to be secure and controlled. Security and privacy weren't part of its original design.

Email contains bits of data you don't usually see. Like code showing what computer sent it, what computer received it, where it travelled along its path, and what time all that happened.

So, nearly all of the email flying around the Internet is unencrypted. Most email providers have no incentive to encrypt the email that passes through their servers.

In fact, companies like Google, make money by showing you ads based on your email content.

The best advice is to treat email as though it were open to the public to read.

Think of email as more like a postcard than a letter tucked safely in an envelope.

Don't say things you don't want others to read, and remember that even after you've deleted your emails, they will be available for years from many other sources.

So this week, when you click Reply All and attach your company's latest earnings report, before you click send, consider who eyes may spy those financials.

Who knows? A bit of caution might just be a good sign.

That's Say What?! for this week. Thanks for listening!

Support for this podcast comes from The Quins. Nominated Boston's Band of the Year in 2019. Check them out at https://www.thequinsband.com/ and on Facebook and Instagram @thequins. That's Q U I N S.