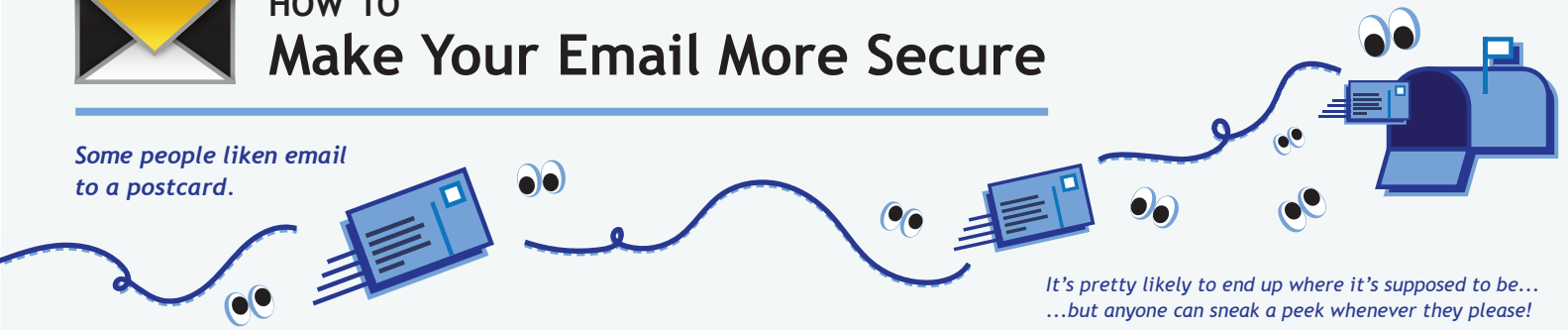




HOW TO

Make Your Email More Secure

Some people liken email to a postcard.



*It's pretty likely to end up where it's supposed to be...
...but anyone can sneak a peek whenever they please!*

01 Remember that email isn't always secure.

Your message doesn't travel down a direct path as you might think, but rather makes multiple stops along the way. The trick is to always make sure you know exactly where your email is going and who is going to read it.

02 Make a strong password and change it regularly.

Always use at least 8 characters and a mix of upper and lowercase letters, numbers, and special characters. Don't use common words or phrases, and never use your name. Remember that anything that makes your password easier to remember also makes it easier to hack.

03 Never reuse your passwords.

Passwords can be hard to remember, but you must fight the urge to use the same one for every account. It may seem convenient until one gets hacked and they all become vulnerable. Keep in mind that a common way for criminals get access to your important stuff is to hack the easier, not as important stuff first.

04 Only transmit information over encrypted channels.

SSL (Secure Socket Layers) is the standard for ensuring a secure connection from your browser, email client, or any other tool. If you're using a browser, check for the "locked" image beside the url; if you're using an email client, make sure you've selected an SSL or TLS (Transport Layer Security) connection. If you're not sure about your connection status, ask your ISP.

05 Use tough security questions.

If you create your own questions, make the answers as obscure and random as possible. If not, use false answers; you'd be surprised to learn how much information about you can be found online or even just guessed. Just make sure that your answers aren't so off-track that you forget them yourself!

06 Use a good virus checker.

Your device can become infected in any number of ways. Once your account is compromised, that's it. Using information they find there, not only can they corrupt and destroy your files, they employ a variety of techniques to steal your information, including watching your keystrokes to steal your passwords.

07 Be aware of phishing attacks.

Phishing attacks are emails that seem innocent, but then ask you to click on a link or ask you to download an attachment. It's important to always pay attention to tell tale signs, such as unofficial or misspelled addresses (always make sure the email address matches the sender name), and never click or download anything from anyone you don't know.

08 Update your software regularly.

Failure to install updates in a timely manner can leave you open to huge security risks, not to mention bug fixes and improved functionality. Hackers will always sniff out holes and other vulnerabilities in a program's code, especially once an update is released and these exploitable entry points become public knowledge. Remember, good security starts at home.

09 Read and understand your email provider's Terms of Service.

The TOS given by your email provider will let you in on important information about which security measures they have in place and what you need to take care of yourself. While you may think that they have your best interests in mind, there's a good chance that their definition is very different than yours.

10 Check out your ISP's email service.

Usually, your ISP will have their own webmail option for you to use, and you might be surprised at what advanced tools are available. For instance, they might allow you to only permit access to your account via secure connections or through certain services, devices, or countries.

11 Never give out login information. Ever.

It may seem obvious but it is by far the easiest and most effective way to keep your account secure. Your friends and family don't need access, and never will there ever be a legitimate service or company that will require you to provide your login credentials – those guys are never up to any good.

brought to you by the makers of MagicMail
www.magicmail.com info@magicmail.com