# If You Want To Protect Your Privacy, Secure Your Gmail

Suppose you are one of hundreds of millions of individuals who use a webmail account (Gmail, Hotmail, Yahoo!, AOL, etc.), and you access this account at an Internet café. Later, you find out that your webmail account has been compromised — someone has read your mail, downloaded files you have stored, and sent messages claiming to be you. But you have always taken precautions with your password, so what could have happened?

It may be that the wireless signal from your computer was compromised. Easily available software makes it possible for hackers to intercept these signals. If you are using an online service, such as webmail, a hacker may then be able to find pieces of data called "authentication cookies." It will sometimes be possible for these cookies to be re-used by the hacker, allowing him or her access to your webmail account. So, given that information, what can you do?

On a public network, there is little that you can do to prevent your computer's wireless transmissions from being intercepted. What you can do, however, is ensure that any intercepted data can't be read, understood or used by a hacker or malicious individual. This will typically be done through encryption — a means of coding a message so that only the intended recipient will be able to understand it.

## How to Encrypt Your Gmail

Unlike most major webmail providers, Google's Gmail provides users with the option to encrypt all communications through their website (other providers will generally protect only log-in information). The method of encryption used is SSL (Secure Socket Layer), which is the same form of protection used by the banks for e-banking services, among others.

Using Gmail's SSL capabilities requires no expertise on the part of the user; all you have to do is turn it on, using one of the two following simple procedures:

*To turn on SSL for a single session:*

- In your web browser's address bar, type an "s" after http ("**https**://mail.google.com", instead of "http://mail.google.com".)

*To turn on SSL for all future sessions:*

- After logging into your account, click the "**Settings**" link in the top-right corner of the screen.

- Change the last setting on the page, called "Browser Connection" to "Always use https".

- Hit the '**Save Changes**' button, and refresh your browser to begin using SSL.

## What is SSL?

SSL, or the Secure Socket Layer, is a way in which personal or sensitive information is protected when being transferred through the Internet. When you visit a website that uses SSL protection, a connection is established between the site and your browser, allowing all communications between the two to be encrypted, rendering them unreadable by any other person or computer.

SSL is a common Internet standard, and is incorporated into all current popular browsers. E-banking websites and e-commerce checkouts usually utilize SSL to protect your financial transactions. You are generally not required to take any action to protect yourself on these sites; if SSL is used by the website, your browser will automatically establish a secure connection.

There are two ways to recognize whether a webpage is protected by SSL. The most obvious sign is that the URL of the page will begin with "https" (note the added 's') instead of the standard "http". Additionally, a 'lock' icon will generally appear on the web browser, though the location may differ depending on the browser you are using: the most recent version of Internet Explorer displays this in the address bar; Firefox in the bottom right corner (in the status bar); and Safari in the top right (above the address bar). However, no matter which browser you are using, you can always click on the lock icon to get more information about the site's security.

## Why do you need SSL?

When information is sent to the Internet from your computer (or vice versa), it may be intercepted, regardless of what form it takes. The important factor to consider, though, is whether the intercepted information can be understood or re-used by another individual. Encrypting information that is being transmitted is one way to prevent this, by changing the data into a form that is meaningful only to the intended recipient. This is the protection that is offered by SSL.

As stated previously, many sites that transmit personal information – particularly those dealing in financial information — encrypt their transmissions, by default. Logins for most online applications are also commonly protected by SSL. However, many sites also use "authentication cookies" to keep track of a user's current session. If left unencrypted, these cookies can be intercepted and used by a hacker to access that user's account. In the context of webmail, this may mean that another person can read, modify, delete or create new e-mail messages. As webmail becomes more popular, the risk of damage increases due to individuals storing sensitive information or documents; identity theft is also a growing concern in this situation. Encrypting data through SSL communications significantly mitigates these possibilities.

**Information and Privacy
Commissioner of Ontario
CANADA**
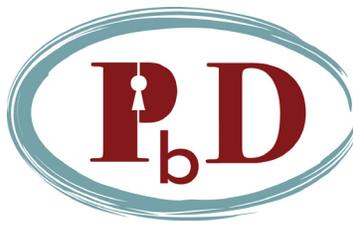
# SSL and Privacy by Design

SSL is a Privacy Enhancing Technology that has been available since the mid-1990s. The IPC would ideally like to see SSL protections enabled as the default option in Gmail, a change which Google has stated that they are investigating. However, the IPC does commend Google for including SSL in the architecture of Gmail, and hopes that all other webmail providers will follow suit. Users should look for strong privacy and security features when choosing a service. The presence of such 'designed-in' privacy features allows you, the user, to choose your security settings, as you see fit. This is the philosophy behind *Privacy by Design*: when privacy features are embedded directly into the system, thereby being present from the outset, user data is more strongly protected, empowering users in the process.

*Privacy by Design* was a term developed by Dr. Cavoukian in the '90s, in an effort to enlist the support of technology to *protect* privacy, rather than encroach upon it. By embedding privacy into the design of various technologies, and actually building it into the architecture of the technology involved, privacy is far more likely to be protected, instead of being viewed as an afterthought.

Organizations may employ "Privacy-Enhancing Technologies" (PETs), or better still, what Dr. Cavoukian now calls, "PETs *Plus*" to achieve their privacy objectives in a positive-sum (not zero-sum) manner. Over the years, she has shone the spotlight on many promising PETs in an effort to raise greater awareness, and to support their development and widespread adoption. Concepts such as PETs, when combined with a positive-sum paradigm, can effect transformative change – transforming privacy problems into privacy solutions. The result: "Transformative Technologies."

## Ann Cavoukian, Ph.D.

**Information & Privacy Commissioner**
**Ontario, Canada**