

# ONE<sup>®</sup> Mail Security Best Practices For OntarioMD Portal Users

Document Identifier: OM-SBPP  
Version: 3.00

## Copyright Notice

This document is copyright of eHealth Ontario.

### All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

### Trademarks

Product names mentioned in this document may be trademarks or registered trademarks of eHealth Ontario and other respective companies and are hereby acknowledged.

### Revision History

Date	Version	Revision
Feb 2009	3.0	Updated embedded SSHA references to eHealth Ontario; updated Address Book nomenclature to harmonize with OMD Portal
Nov 2008	2.0	Updated template, logos, and organization name from SSHA to eHealth Ontario
Oct 2005	1.0	Initial release

### Authorized Reader

This document is authorized to the following organizational roles:

#### Role(s)

---

- End Users

## Table of Contents

---

1.0	About this Document .....	4
1.1.	Document Approach and Scope.....	4
1.2.	Audience .....	4
1.3.	Assumptions.....	4

---

2.0	Overview .....	5
-----	----------------	---

---

3.0	Best Practices using your ONE Mail Account .....	6
3.1.1.	Your Computer .....	6
3.1.2.	Accessing and Viewing Email .....	6
3.1.3.	Attachments.....	7
3.1.4.	General.....	7

---

4.0	Appendix A – Glossary .....	8
-----	-----------------------------	---

## About this Document

### ***1.1. Document Approach and Scope***

ONE Mail is a service provided by eHealth Ontario.

This document provides information on the safety and security practices one should employ when using ONE Mail services.

### ***1.2. Audience***

This document is intended for healthcare providers that are registered with the OntarioMD Portal and who are enrolled users of the eHealth Ontario ONE Mail service product.

### ***1.3. Assumptions***

This document assumes the following:

- The reader is familiar with using an e-mail application.

## 2.0 Overview

What is **ONE Mail Security Best Practices**?

- **ONE Mail Security Best Practices** - is a common sense approach to using an e-mail account in a safe and secure manner. It provides awareness for those who rely on the use of e-mail in the running of their day-to-day business practice.

## 3.0 Best Practices using your ONE Mail Account

To apply best practices, we have provided you with the following breakdown. These specific component areas will assist you with the understanding of how you can have a safe and secure email environment.

Applying and using best practices ensures a high degree and level of comfort in the use of ONE Mail services.

### 3.1.1. Your Computer

Apply individual user accounts to your computer and don't share your account information.

Do not use unencrypted wireless communications with patient-identifiable information.

Use antivirus software and keep it updated.

[Use spam filters](#) to help block unwanted e-mail, much of which contains dangerous attachments.

**Use password-protected screen savers for all desktop workstations in the office, hospital, and at home.**

**Enable personal firewalls on your computer, in a large environment implement a firewall appliance between the internet and your computer network.**

Set up your office network securely to protect health information against any security threats such as unauthorized access.

Ensure that browsers (e.g. Explorer, Netscape) and operating systems (e.g., MS Windows) are up-to-date and that security patches are applied.

### 3.1.2. Accessing and Viewing Email

Being aware of where you are, especially when viewing sensitive information. Sensitive information should not be viewed where others may be able to see your screen.

Be suspicious of any e-mails with requests for personal, financial, or sensitive information that may attempt to take you to another website to enter the information or reply to the sent email.

Use caution with links supplied in e-mails. Do not click on links in e-mails if you suspect that the message might not be authentic (i.e., if you don't recognize the sender or understand the subject or message).

Caching within Internet Browsers may retain residual information others can access, these should be cleared through the use of browser tools

When viewing an e-mail, don't open any attachment unless you know whom it's from *and* you were expecting it.

When viewing an e-mail, if you receive an e-mail message with an attachment from someone you don't know, delete it immediately as it may contain harmful viruses.

### 3.1.3. Attachments

Attachments saved on a local computer are outside of the ONE Mail secure messaging infrastructure. Ensure you protect any saved copies of attachments with sensitive content as you would protect paper records

When including Personal Health Information attachments within an e-mail message, ensure you recognize and follow all Privacy and Security guidelines and legislations as you would for paper documents.

If you need to send an e-mail attachment to someone, let them know you'll be sending it so they don't think it may contain a virus and delete it mistakenly.

See "Accessing and Viewing Email" section 3.1.3 above for viewing e-mail with attachments for further information

### 3.1.4. General

Ensure your staff read and follow these best practices.

Establish turnaround time for messages. Do not use e-mail for urgent matters.

There is no real protection from misuse of the e-mail service (e.g. sending an email to a Hotmail account)

Healthcare providers are responsible for the security of the personal health information in their custody/possession when embedded within e-mail messages. The end user is responsible that the technology is used appropriately. Apply Privacy and Security policies as applicable by law under such circumstances.

Security of email is dependent on an adequate degree of assurance of the identity of the sender and recipient – i.e. each party should know who the other communicating party is

Communicate by e-mail only information you are comfortable having forwarded.

Avoid using e-mail for time sensitive messages.

Avoid using e-mail for sensitive matters.

Always report 'phishing' e-mails to the organization first. Users can report incidents to local law enforcement agencies to officially open an investigation.

## 4.0 Appendix A – Glossary

Term	Definition
phishing	Used to describe a scam whereby an e-mail is sent to an end-user with the representation that the e-mail comes from a legitimate establishment; but the true intent is to gather personal information from the end-user for fraudulent use.
Recipient	An individual who is the selected or anticipated receiver of an e-mail message and/or any attachments. In the e-mail message header information it is referenced by the fields <b>To:</b> or <b>CC: (Carbon Copy)</b> or <b>Bcc: (Blind Carbon Copy)</b>
Sender	An individual who is sending or has sent an e-mail message. In the e-mail message header information it is referenced by the field <b>From:</b>
Spam	To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. From the sender's point-of-view, it's a form of bulk mail, often to a list culled from subscribers to a discussion group or obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail.