DON’T BE AN INTERNET TURKEY

4 Simple Ways to Secure Your Email

Hacking someone’s e-mail address promises potential rewards for the criminally-minded. Of course, the most obvious is gaining access to your private conversations, whether to reveal sensitive personal or professional, information that could be used for malicious purposes including identity theft and corporate espionage. A hacker could also delete messages in an attempt to destroy valuable information.

But for the average online user, the most serious threat from hacked e-mail is that a criminal can use your account to discover the keys to your other online accounts, such as financial services like banking and PayPal. Many websites with secure login portals provide the ability for you to retrieve a “forgotten” username and/or password. When the sites send this information to your registered e-mail account, it is presumed that you are the only one with access to this account. A hacker who has snuck in could do the same, and gain direct access to everything from your Facebook account to your mortgage, investments, banking, and utilities.

These four lessons in email safety can help protect your business and your personal email from attack:

1. **Put your "eggs" in several baskets.**

Considering that e-mail addresses are easy and often free to acquire, dilute your risk by spreading your inbox exposure. For example, using a separate e-mail address for work and personal correspondence keeps sensitive professional details in a separate place from a hacker who might break into your personal account.

Better yet, keep separate addresses for secure and unsecure website registrations. Most of us wind up registering with dozens of websites, but only some of them relate to sensitive information like banking. Many others are simply Web communities like message boards and funny cat pictures. Using a different e-mail account for secure sites will prevent hackers from impersonating you to gain access to those sites if they hack into the account you use for leisure sites.

E-mail readers, including Outlook, Windows Live Mail, Thunderbird, and Apple Mail can be configured to check multiple accounts simultaneously (including Gmail), to minimize the inconvenience of keeping tabs on separate accounts.

2. **Secure against sniffers**

   In hacker's parlance, a "sniffer" is any kind of software that can intercept data as it moves across the network. Depending on the security of the network itself, it can be possible to sniff both wireless and wired connections. Sniffing can be especially useful for plucking out login and password information as it travels across the network.

   The best defense against sniffing is to encrypt the data—this way, all the hacker will see is garbled and useless. When using e-mail there are several layers to consider:

   Web-based e-mail: when reading e-mail using a Web interface, such as Gmail, Yahoo Mail, or your service provider's own webmail reader, be sure to use an HTTPS connection rather than just HTTP.

   When visiting your webmail, look at the URL in the address bar and check that it begins with *https://*. Many browsers will also display a lock icon when connected to a secure site, such as shopping and bank sites. If your webmail does not use https, try typing it in manually; if that doesn't work, your provider may not support a secure connection, which should give you pause: using webmail over a plain HTTP connection leaves your login and message content exposed to network sniffers.

   E-mail clients: if you use an e-mail reader, such as Outlook or Apple Mail, you can configure these clients to connect securely. When you setup your accounts, you would have selected either POP or IMAP connections—both can be performed in secure mode, which should be an option in your account configuration (exact details and wording may vary).

   Note that secure POP and secure IMAP only encrypt the login itself—in other words, your username and password to the e-mail server. These protocols do not encrypt the actual message content.

   Your e-mail client may also provide the option to use TLS, or Transport Layer Security. TLS is basically the e-mail equivalent of HTTPS, meaning that it encrypts all data passing across the network between client and server. It is important to remember that TLS does not encrypt your e-mail inbox—in other words, the messages in your inbox are not encrypted and anyone with access to your e-mail account can view them. TLS simply encrypts the messages while *in transit*.

3. **Use webmail with caution**

   The maturation of webmail services, such as Gmail, Yahoo Mail, and even Outlook Web Access, encourage convenient e-mail usage anywhere there is a Web browser. This can be a blessing and a curse.

When using webmail on public computers, such as at a library or campus terminal (or even simply borrowing someone else's machine), it is important to avoid leaving behind digital footprints.

The most obvious defense, of course, is to remember to log out of your webmail before walking away from a terminal. Even the most cautious of us can sometimes forget this simple step, especially when distracted by our iPods and iPhones--and iEverything.

But simply logging out **may** not be defense enough against a savvy hacker. A clever hacker could walk up to that machine and quickly, discreetly copy the browser's history and cookies to a thumb drive, to be analyzed later for any useful tokens or hints to the webmail accounts that were used. While these records won't contain your actual passwords, they could provide enough information to serve as a starting point.

Closing the Web browser after your webmail session is a good idea. This should flush some if not all of these records. Better yet, switch the public browser to private mode before connecting to webmail. Not all browsers support "private browsing" mode, but many now do and you can find simple instructions for Firefox, Internet Explorer, and Safari. Remember to exit private mode at the end of your webmail usage and the browser will destroy any history or cookies associated with your session.

4. Keep a clean Operating System

We haven't yet talked about your e-mail account password. Of course your password should be anything less than blatantly obvious (like all zeroes or repeating your username or, heaven forbid, "God"). Fact is, it won't make any difference how "strong" your password is if your computer is infected with malware that intercepts it right out of your hands.

And that's the bigger problem today—malware from infected software and drive-by downloads that can install keyloggers and other sorts of sniffers on your PC grabbing your passwords as you type (or save) them.

So really, the best defense to secure your e-mail passwords is less the passwords themselves and more that you keep a clean OS. This means you, Windows users. Aggressive deployment of resident malware scanners, such as Windows Defender, Windows Security Essentials, or third-party tools including AVG, Avast, Spybot Search and Destroy, or Malwarebytes, will reduce your chance of being infected by password-stealing malware.

5. Conclusion

If you take nothing away from this article but one point, it is, if you are **UNCERTAIN IN THE LEAST**, **DO NOT CLICK** and **DO NOT OPEN ANYTHING**. A quick email (fresh, NOT via the reply method to the sender) to clarify the email takes but a moment.

Having your computer corrupted can spread the pain to many others, and cost you time and money as the techs at Best Buy fix the problem.

Hint

Make your Subject Line personal. “Cute”, I won’t even think before deleting, “Cute Pictures From The Gingerbread Event”, I will have a look at.

Russ Pastuch
Chair, Communications Committee