

Re: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-10/msg00207.html>

- *From:* Kenton Smith <listsks@xxxxxxx>
 - *Date:* Tue, 17 Oct 2006 15:03:56 -0700 (PDT)
-

I think they're all worth considering (or I wouldn't have sent them).

My comments were intended to be very general because the original poster was very general in his request for information. Of course an unsecured mail server is not going to be any better than a public mail server.

However I was basing my comparisons on using a public mail server vs. a correctly secured and configured private mail server. I would hope that if a company was considering the security of a free mail service, they'd do the same if they were implementing their own corporate mail server.

----- Original Message -----

From: "Hagen, Eric" <hagene@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

To: Kenton Smith <listsks@xxxxxxx>; sfbmailsbm@xxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxx

Sent: Tuesday, October 17, 2006 2:37:00 PM

Subject: RE: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

A few of the points you bring up are not entirely accurate, but at least one is worth considering.

First of all, keep in mind that a return address pointing at "a domain you control" does not mean anything. Unless your customers are going to pick apart the email headers and trace the SMTP route of the mail back to your servers, this is a false security. Anyone willing to create a hotmail account and impersonate your company can just as easily fake your return address from almost any standard SMTP mail client.

Unless of course, you're using some sort of encrypted signature to verify your identity, in which case, it doesn't matter the provider you use.

The encryption issue is also a red herring, simply because your company's POP3 or Exchange email is also sent cleartext over the wire. Frankly, it is far easier to secure a webmail session (put an https in front of it on most servers) than it is to secure a POP3 session. In addition, login passwords are ALWAYS transmitted with SSL for webmail clients, whereas POP3 defaults to transmitting cleartext passwords.

The only real issue that you mention is the potential conflict of housing sensitive customer data on third party servers. This is an issue that must be addressed and can only be determined on a case-by-case basis. An advertising rep who receives ad copy via email is not jeopardizing the business by exposing this to a third party, since it is generally not extremely sensitive data, however an HR rep from the same company who sends emails about an employee's salary and benefits might be in violation of company policy, not to mention the law.

Eric

Re: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx] On Behalf Of Kenton Smith
Sent: Monday, October 16, 2006 4:32 PM
To: sfgmailsbm@xxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

Big risk! Here are a few off the top of my head.

The number one risk of using these sites is that communication tends to not be encrypted. That means anyone sitting in the same wireless equipped cafe can easily intercept and read all email communication.

Also, depending on the regulatory requirements of your business it may be illegal to be storing customer sensitive data on a third-party server over which you have no control.

Lastly, and of less importance (maybe) is that there is no way to prove that a person has any authority to represent your company. At least if the mail is coming from a domain you control a prospective or active client can be reasonably assured that you are who you say you are. Of course there are better ways than just having an email address. But I think that if your users are currently using public mail providers for business email, certificates and email encryption aren't high on the company's list of priorities.

Kenton

----- Original Message -----

From: "sfgmailsbm@xxxxxxxxxxx" <sfgmailsbm@xxxxxxxxxxx>
To: security-basics@xxxxxxxxxxxxxxxxxxxxx
Sent: Monday, October 16, 2006 12:00:16 AM
Subject: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

Dear List,

It is a common practice among users to use their personal email accounts like hotmail, gmail, etc to send & receive business (and most probably confidential) information

This is particularly the case when users are out of office

These webmails are not under the company's control, and hence there is a risk of information loss. However upto now we have not heard of any such cases

Wanted to get the opinion of the list on the security risks of the use of Webmails for business mails

Thanks & regards

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

Re: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

Re: Using Web mail (hotmail, gmail, yahoo, etc) for Business mails

The NSA has designated Norwich University a center of Academic Excellence in Information Security. Our program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience. Using interactive e-Learning technology, you can earn this esteemed degree, without disrupting your career or home life.

<http://www.msia.norwich.edu/secfocus>

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The NSA has designated Norwich University a center of Academic Excellence in Information Security. Our program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience. Using interactive e-Learning technology, you can earn this esteemed degree, without disrupting your career or home life.

<http://www.msia.norwich.edu/secfocus>

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The NSA has designated Norwich University a center of Academic Excellence in Information Security. Our program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience. Using interactive e-Learning technology, you can earn this esteemed degree, without disrupting your career or home life.

<http://www.msia.norwich.edu/secfocus>
