March, 2019

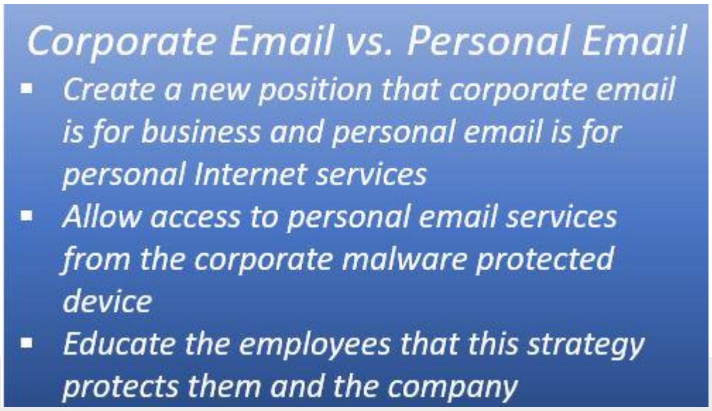
Renaissance IT Consulting, LLC

Technology Insider

Risky Business

When I visit my clients and conduct my IT security assessments, I make it a point to review the company’s security strategy for corporate email and personal email. I find conflicting strategies in place, and often very strong-minded opinions on what should be allowed and what should be blocked.

Some companies block employee’s access to personal email websites such as Yahoo and Gmail due to the threat of employees clicking on unsafe emails. Since they have email filtering on their corporate email, they feel the machines and network are safer if the employee can’t access their personal email on their company-provided PC. Digging deeper, I find that employees facing this challenge, begin to use their corporate email id as their user-ids for personal internet services such as Amazon, Apple, LinkedIn and TurboTax. They do this so they can get order confirmations, shipping notifications and other emails delivered to them while they are working and using their company computer. Some employees even use their corporate email ID for login into their on-line banking accounts.



Corporate Email vs. Personal Email

- *Create a new position that corporate email is for business and personal email is for personal Internet services*
- *Allow access to personal email services from the corporate malware protected device*
- *Educate the employees that this strategy protects them and the company*

What’s the Risk?

There are several reasons why using your company email for personal use on the Internet is a bad idea. Hopefully you can find some arguments here to share with your employees and your IT staff to improve your email posture while facing potentially unsafe employees.

There are usually only two reasons why employees use their company email for personal use – 1.) IT is blocking access to personal email sites, and 2.) it’s convenient to get all my email in one place. Here’s why it’s a bad idea:

1. Your personal email may be stored or archived per the company’s email retention policy – potentially forever. It will also be subject to eDiscovery searches and disclosures. If you don’t want your email to end up in court filing, don’t use the company email. This practice also increases the amount of email the company must save – increasing company storage and backup costs. Many companies limit mailbox sizes, forcing the user to create PST’s which also create a costly storage environment.
2. Your personal email should be private and corporate email is not private. The company has the right to access your email and can do so if they suspect anything suspicious or if requested by a supervisor or Human Resources manager. If you were job searching, or planning to start your own business, this email could be easily accessed during one of these investigations.
3. Registering your corporate email with Internet forums or services increases the amount of SPAM your company’s email system must deal with. More importantly, the company email gets on more and more lists, exposing the company to more breaches.
4. It increases attacks against the company and can lead to successful attacks of corporate resources. When an Internet email list is compromised, user and password combinations can be acquired and used against other services. Hackers will immediately start trying the same user-id/password combinations against your corporate email account and other corporate services such as cloud systems.
5. This practice creates a problem if you decide to leave or are asked to leave your employment. You will lose access to your email account immediately upon exit, and although you might be able to copy personal email, a copy of these emails remains on the server. You will be forced to change your account name or email address on all personal Internet services (hopefully you remember which ones are in use).

6. Companies with employees in Europe are dealing with the new GDPR regulations. Using company email for personal services increases the responsibility of the company to protect, remove and return personal email when an employee leaves the company.

What Should Corporations Do?

Company IT and IT Security managers should meet with their legal and compliance executives and work together to implement a new strategy. It's very possible that the executives have not considered the threat to be great enough to create and publish a new position. Company's recovering from cyber-attacks will wish they had addressed this earlier.

1. Make and publish a policy that clearly defines how corporate email is to be used. Be clear on the position of the Company Internet Profile vs. Personal Internet Profile.
2. Allow access to personal email providers through your corporate web filter. The old philosophy of employees spending too much time doing personal email is outdated and overly restrictive given today's digital age. Blocking employee's access to personal email won't suddenly make them "star" employees. Supervisors can manage employee's productivity, not corporate email systems.
3. Enable firewall tools to black-list and block email and other traffic from domains that are potentially damaging and clearly not related to your business. Where possible, enable credential reuse blocking – preventing the reuse of your main credential on 3rd party sites.
4. In addition, corporations should technically implement a policy that prevents auto-forwarding of corporate emails to off-site email addresses. There are many risks to the company when employees do this. Personal email should never be used to conduct corporate business.

In summary, this digital age is exploding in the consumer space and keeping the business safe from employees who easily wander into many new Internet services is critical. There should be a distinct separation between a person's company Internet profile and personal Internet profile – and the two should not be mixed. It's better for the employee and better for the company.

Chuck Maiorana
Renaissance IT Consulting, LLC
Shelby Twp., MI 48315

248-274-4480
cwmaiorana@renaissanceitconsulting.com
www.renaissanceitconsulting.com