Peter Rose
Mar 4, 2015
to me
Same rules apply today as did 100 years ago. If you don't want to see it in the morning paper, don't put it in writing in the first place. The internet is for spreading information, not for keeping secrets.

On Wed, Mar 4, 2015 at 10:52 AM, Emily Rose <rose_emily@wheatoncollege.edu> wrote:
Awesome. Thanks so much!! That's pretty similar to what Wheaton has transitioned into, so it'll be great to compare the two.

Emily S. Rose

Wheaton Equestrian Captain & Treasurer
Archives Assistant
Wheaton College '15

On Wed, Mar 4, 2015 at 10:26 AM, Peter Rose <prose@uri.edu> wrote:
Before January 6th of this year,
To the best of my knowledge, (which may be incomplete), the only regular
"monitoring" URI did of employee or student mail uses automated systems that
(1) attempt to detect outgoing spam, and
(2) (some? all?) employee mail is filtered to attempt to detect whether they're sending
"sensitive data", meaning social security numbers.

In the first instance, the email account is simply shut off*, until the user contacts us,
and in the second, the offending email is bounced back to the user with a message
that says something like: "This looks like it's got sensitive data in it, which you're not supposed to send by mail. Are you sure you want to do this? If so, do X, otherwise, this message will not be delivered."

In neither case is the email looked at by humans. In cases involving a court order
or (I think) a request by the head of Human Resources Administration, mail administrators can go into a user's email account to look for evidence of criminal activity or violation of policy, in which case humans DO end up looking at your stuff.

Since January 6th of this year, URI has outsourced it's standard employee email accounts to gmail, which means that we can't get into your email without re-setting the password anyway, and we depend on gmail to filter for spam. So whatever vulnerabilities you have with your regular gmail account, those are the ones that apply to your uri.edu email account.

There are several departments that maintain their own email servers, and as far as I know, the old rules apply to those.

Of course, if we really wanted to, we could use various network analysis and monitoring tools to capture *ALL* network traffic, ingoing or outgoing, to and net-device registered in your name. We just don't, because nobody cares enough.

On Tue, Mar 3, 2015 at 1:56 PM, Emily Rose <rose_emily@wheatoncollege.edu> wrote:
Hi Uncle Peter!

I am writing a research paper for my computer science senior seminar on the policies and practices of employee email privacy in higher education and I was wondering if you have any information about how URI handles the subject? I found a few different resources on the URI website, but if you are willing to share any personal experience or opinions on the matter, I would be very grateful.

Thanks!
Emily S. Rose

Wheaton Equestrian Captain & Treasurer
Archives Assistant
Wheaton College '15