Concerns regarding Proofpoint at URI

Dept. of Computer Science and Statistics

Introduction

At some point during 2019, URI enabled Proofpoint as an email filtering service, without the ability for users to opt out of this service.

Proofpoint implements several modes of operation: "spam" filtering, "data loss prevention," and "URL defense." All three of these interfere with normal email operations in some way. Spam filtering redirects some messages to a spam holding area without delivering them, while other messages are marked as spam but delivered; a digest summary of such quarantined emails is delivered periodically. The user can click on this link to mark messages as not spam, but cannot do large batch operations.

Data loss prevention is designed to prevent sources of personal data leakage, such as sending credit card numbers in plain text. It is unclear whether this sort of threat was a real, extant problem at URI, but it now results in messages being deleted with no notice to the recipient.

URL defense consists of all emails inbound to `@uri.edu` addresses having their contents rewritten, such that every URL is replaced with a `urldefense.proofpoint.com` URL with an encoding of the original URL. The ostensible purpose is that these URLs can then be blocked if they are found to be malicious (by what algorithm is apparently a trade secret). Proofpoint's "URL Defense" is designed to prevent attacks such as "phishing" or "spear-phishing"; the former is when a user is tricked into providing sensitive information to a malicious website, while the latter is a customized form where the site may even present plausible pre-populated information about a user, such as a name or email address.

Concerns

We have several concerns with these three "services" that have been imposed on `@uri.edu` email addresses.

False sense of security

Like any machine learning-based filter, Proofpoint's URL defense cannot be perfect. It will exhibit both *false positives,* blocking legitimate URLs, and *false negatives,* allowing access to malicious URLs. Technical users have become used to looking at URLs before following them, and (for instance) typos in a domain name are a major clue that a URL is malicious. Proofpoint's rewriting of URLs removes this first line of defense, to replace it with one where Proofpoint claims all URLs will be safe. Now, however, the ability for users to discern whether a URL might be malicious is lost, and we are unaware of any study indicating whether Proofpoint or manual URL inspection is more effective. Our concern is that users may have a false sense of security, and follow links without question.

Furthermore, the ability to quickly glance at a message and see which URL needs to be clicked on is now diminished. For instance, typical conference or journal referee opportunities have simple URLs which one follows to indicate that one accepts or declines to referee the article. Now, these URLs are not easily distinguished.

Spam filtering imposes a burden

In Proofpoint spam filtering exhibits several problems:

- `uri.edu` addresses are being flagged as spam (and not delivered). These are funding opportunity related emails, as well as other university activities.
- professional association addresses are also being flagged as spam: `ieee.org`, `acm.org`, etc.
- The web interface disallows selecting more than one email at a time to mark as *not* spam.
- The web interface disallows selecting more than five emails as a time to mark as "deliver and allow sender."

We already have spam filtering via the Google-hosted Gmail service, and many of us additionally have spam filtering in our email clients. Proofpoint seems to provide no great benefit here, and imposes significant burdens, including the artificial limitations noted about the web interface, and the fact that internal and professional-organization email addresses seem to be likely to be flagged.

One of our junior faculty members has, as part of her startup package, a membership in the Faculty Success Program (which costs URI $5000 in tuition). This faculty member has missed several email messages from members of this program, even though she has corresponded with these individuals before. She did eventually find the blocked message mentioned in the Proofpoint digest, but clicking "release message" did not actually release the message to her inbox.

Program description:

"The Faculty Success Program is a 12-week, online program that was designed to teach tenure-track and tenured faculty the skills they need to increase both

their research and writing productivity while maintaining a healthy work-life balance. The Faculty Success Program offers an extremely supportive community that works through the day-to-day challenges together, pushes each other when needed, and celebrates each other's successes, big and small. information: https://www.facultydiversity.org/fsp-bootcamp"

According to this faculty member, "The cohort based support is an essential part of the program and so blocking notification e-mails interferes with my ability to engage in a timely manner unless I visit the site periodically otherwise."

Several faculty members have reported that clicking "release" or "release and allow sender" does not reliably cause the email to be delivered.

Another faculty member, the director of our graduate program, has had emails from prospective students flagged as spam by Proofpoint. Quote from this faculty member: "It is actually intercepting legitimate email inquiries from potential graduate students. See the screenshot below. Thus there is potential loss of revenue for the university because proofpoint intercepts these kinds of emails. And this is one that it told me about, who knows how many emails it intercepted without telling me about."

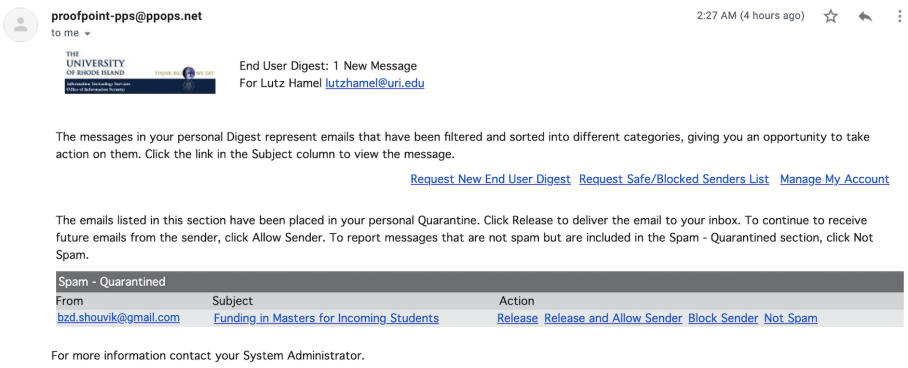

Figure 1: Supposed spam email from prospective student

Some of us have missed funding opportunity notifications due to this filtering.

Unreadability of messages

Proofpoint's rewriting of URLs imposes a significant cognitive burden on users. In a time when we are inundated with emails, more during the pandemic than ever, this is an unacceptable burden. A message with several simple, easily-parsed URLs might normally look like this:

And after Proofpoint's rewriting of URLs, it looks like this:

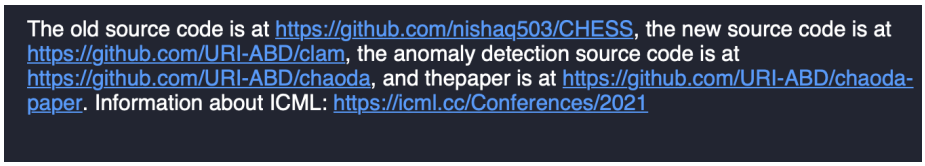

Figure 2: Email message with several URLs with semantic meaning

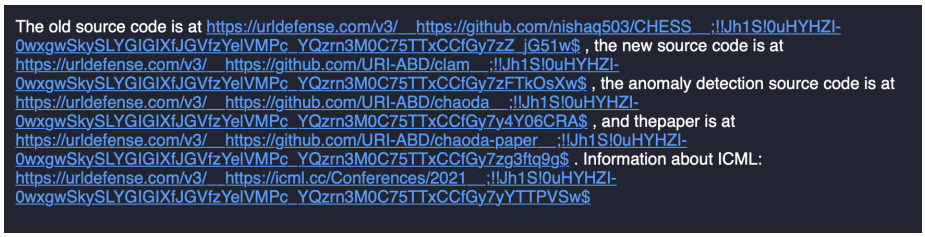

Figure 3: What Proofpoint does to that email message

This makes messages longer, URLs indecipherable, and increases the cognitive burden on users.

Ability for a third party to log web activity

Proofpoint's rewriting of URLs has an additional effect: when a user clicks on a URL, the initial HTTP request goes through Proofpoint's servers. This means that Proofpoint has an opportunity to log our web activity, at least that activity originating from inbound email messages. This poses a serious privacy concern, of which most users are completely unaware.

Loss of research data and undelivered messages

The implementation by Proofpoint is quite problematic, as it has routinely mis-identified messages containing bioinformatics data as instead containing credit card numbers. The behavior when it does so is even more problematic: the message is deleted, with no notice sent to the recipient (though one is sent to the sender). Note that this impacts *incoming* email, not outgoing. While it is unclear whether or not people sending credit card numbers to URI faculty or staff is a significant problem, the silent deletion of research data from a web service hosted at another university is **quite a serious problem.**

Academic freedom

Proofpoint is, fundamentally, *altering communications between academic researchers.* This sometimes results in silent deletion of data, and sometimes results in altering of email messages, but it is nonetheless an unwelcome censor-

ship of communications between members of the academy. An email message from one scholar to another is a carefully-crafted communique, much like a letter. Changing the contents of an email is indistinguishable from altering a letter. This is a violation of the principles of academic freedom.

Conclusion

Proofpoint has constituted a nuisance, without solving any obvious problems. It poses significant problems for scholars, wasting time, making emails less readable, violating privacy, and infringing on academic freedom.

We request that the University address the concerns raised here, at the very least by allowing a way for scholars to opt out of Proofpoint's email manipulations, if not by removing Proofpoint from our email system.