Seems Phishy: Back to School Lures Target University Students and Staff | Proofpoint US

By September 05, 2019 Michael Walsh and the Proofpoint Threat Insight Team

Published: 2019-09-05 · Archived: 2026-04-05 13:20:21 UTC

Overview

Every school year, Proofpoint researchers observe a seasonal uptick in college-themed phishing, especially between June and October, as students prepare for school and near the beginning of the fall term. A typical university phishing campaign is medium volume (thousands or tens of thousands of messages per day). Campaigns are typically not geographically targeted, but rather tied to specific universities with phishing templates developed for library and student management portals. While many of the examples here are from schools in the United States, we regularly observe campaigns affecting hundreds of universities worldwide.

Threat actors distribute messages that contain links or HTML attachments that direct victims to cloned university login portals. These portals incorporate stolen branding, accurate street addresses, and other social engineering techniques to manipulate users into disclosing login credentials.

The fraudulent webpages range in complexity and accuracy compared to the original, but many are indistinguishable from their genuine counterparts. We included several examples of these fake login pages below:

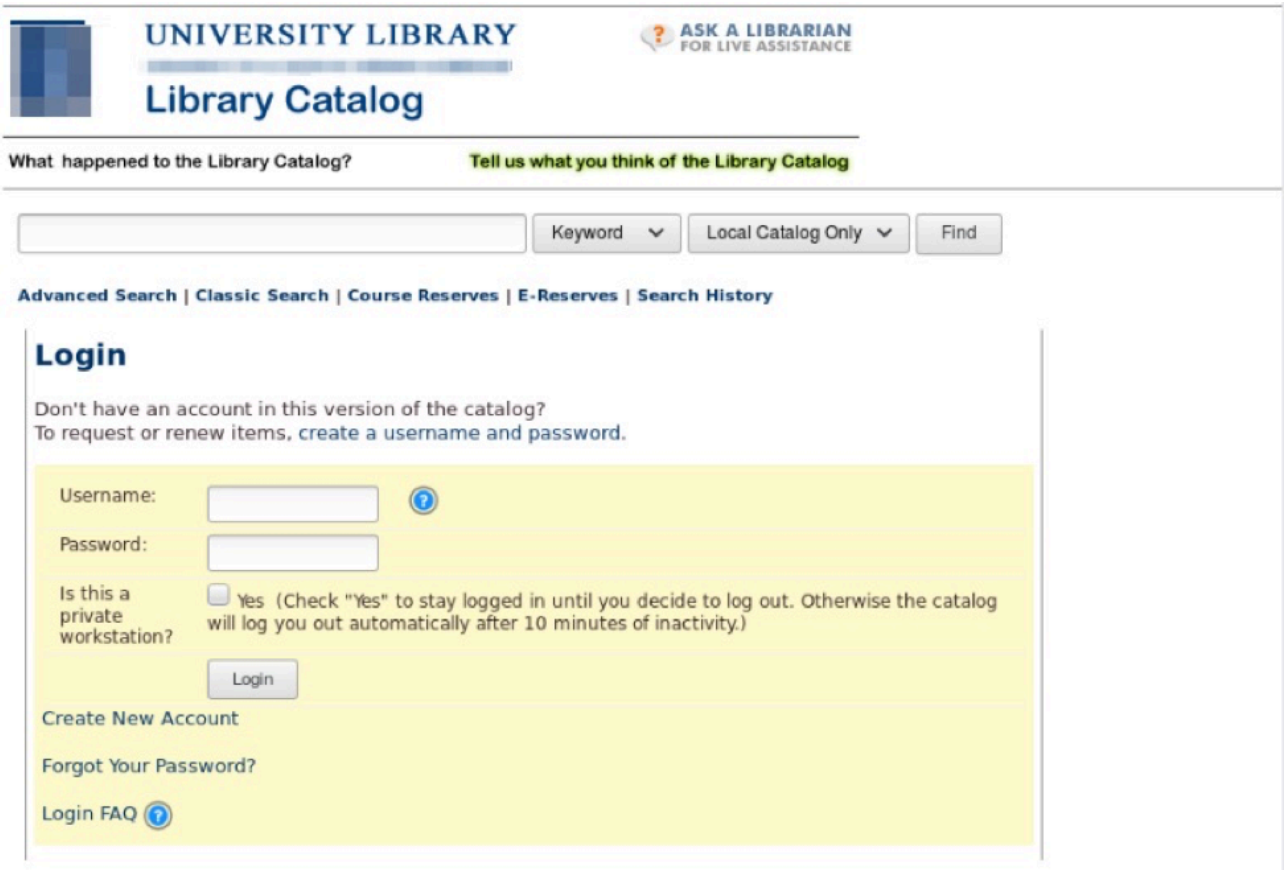

Figure 1: Spoofed university library login portal used for phishing

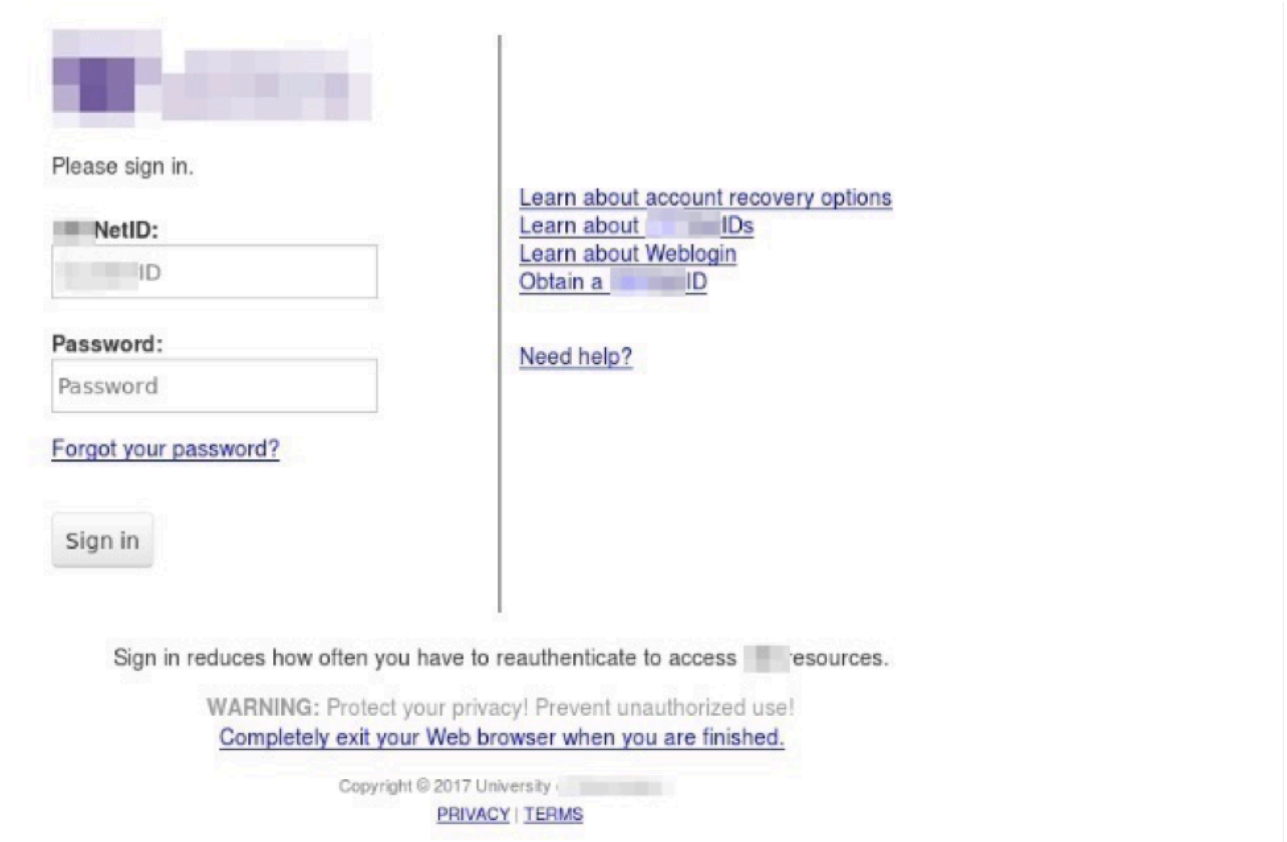

Figure 2: Spoofed university library login portal used for phishing

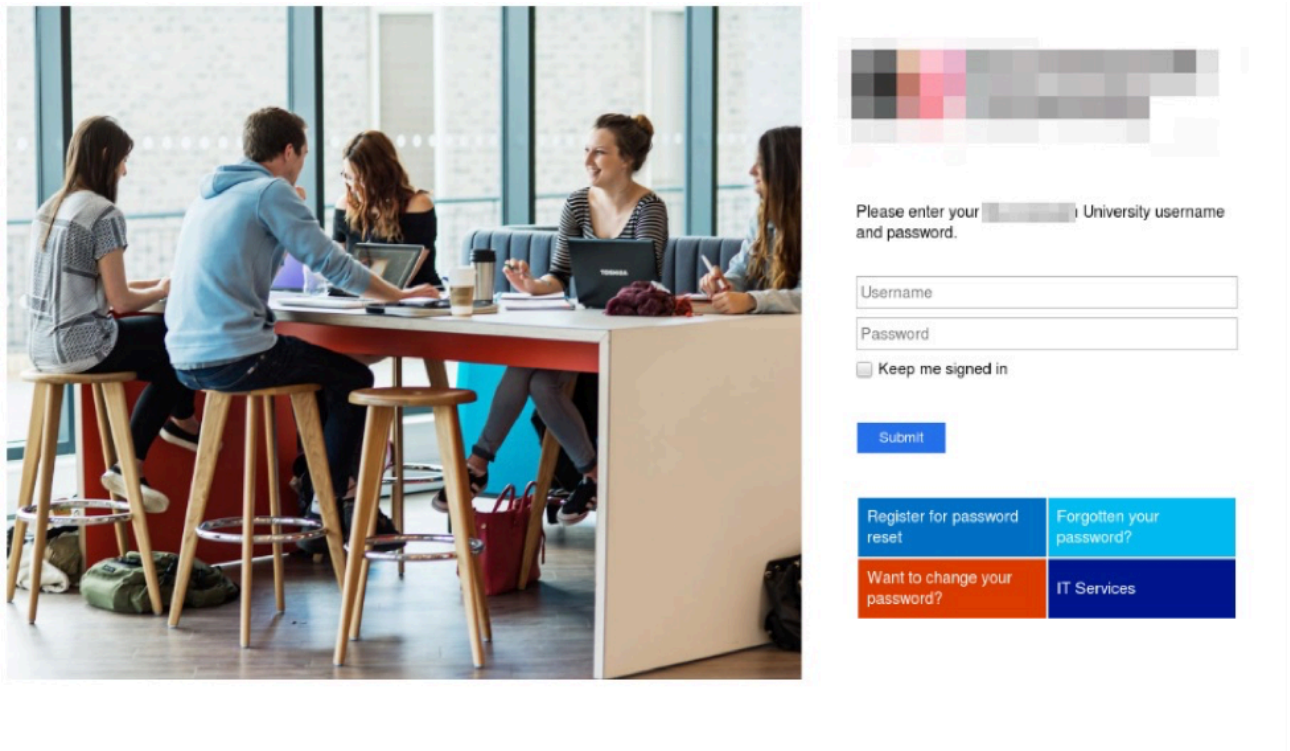

Figure 3: Spoofed university library login portal used for phishing

Delivery

The emails that lead recipients to these phishing portals frequently contain either: (1) HTML attachments with URLs that link to the fraudulent login page, or (2) embedded URLs that link directly to the spoofed portal. The malicious attachments often have generic file names including “new_attached.html”, “ fafsa_2018.pdf”, or “new_rule.html”, some of which, like the Free Application for Federal Student Aid (FAFSA) PDF example, will resonate particularly with students.

After entering their login credentials into the fraudulent login page, victims are often redirected to the genuine university login portal, at which point it simply appears that the login attempt failed. The stolen credentials are then sent to an external site controlled by the attacker, saved in a text file on the same server to be retrieved later, or emailed to inboxes that are controlled by the phisher.

Silent Librarian

TA407, also known as Silent Librarian, is another notable threat for students. The group was indicted by the FBI for its spear phishing campaigns that impersonate university library administration in order to phish for students' login credentials. Ultimately, the group uses these credentials to steal and resell intellectual property, journal subscription credentials, and more.

TA407 primarily targets universities and higher education institutions within the US with low-volume (hundreds or thousands of messages), highly personalized campaigns. These campaigns utilize well-crafted social engineering mechanisms including:

- Stolen branding
- Fake email signatures/credentials/addresses
- Personalized email bodies/portal clones
- Themed subject lines (e.g., “Renewal of loaned items”, “Renew your loaned items”, and “Renewal of materials”)

Since the beginning of 2019, Proofpoint researchers observed several TA407 campaigns distributing phishing campaigns with clones of university library login pages. Although TA407 has made minor variations to its social engineering techniques and infrastructure, their strategies have been rather consistent. Many of these campaigns use the same lures with minor variations in phrasing.

A typical message contains a brief message that warns the student about overdue library materials or outdated library login credentials. The following figures are message bodies excerpted from recent Silent Librarian campaigns:

```
Dear Graduate Student,

Our records show that your access [univ3] library databases is about to
expire. Due to new security precautions established to protect [univ3]
Library system, you have to renew your library account on a regular base,
so please use the following link

Click Here http://go.[univ2].edu/[shortened]

After your successful authentication, your access will be restored
automatically and you will be redirected to the library homepage. If you
are unable to log in, please contact the library help desk for immediate
assistance. We apologize for any inconveniences this may have caused.
```

Figure 4: Silent Librarian email message body template

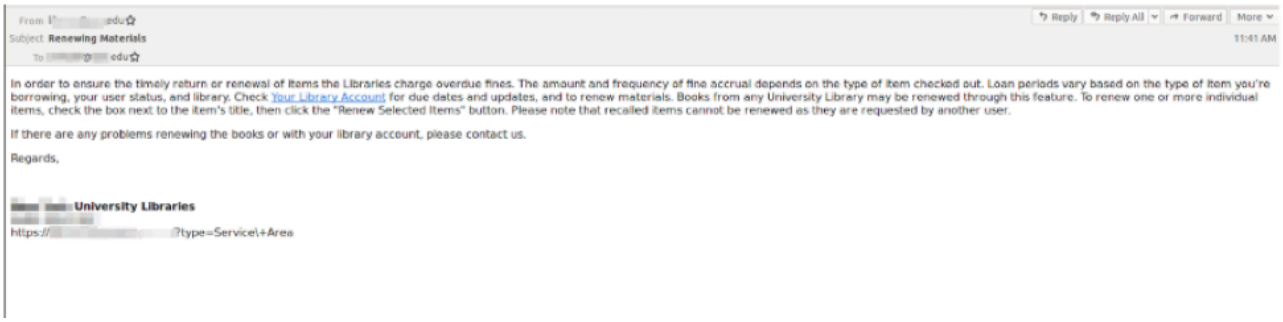

Figure 5: Silent Librarian “Renewal of Materials” message from early 2019

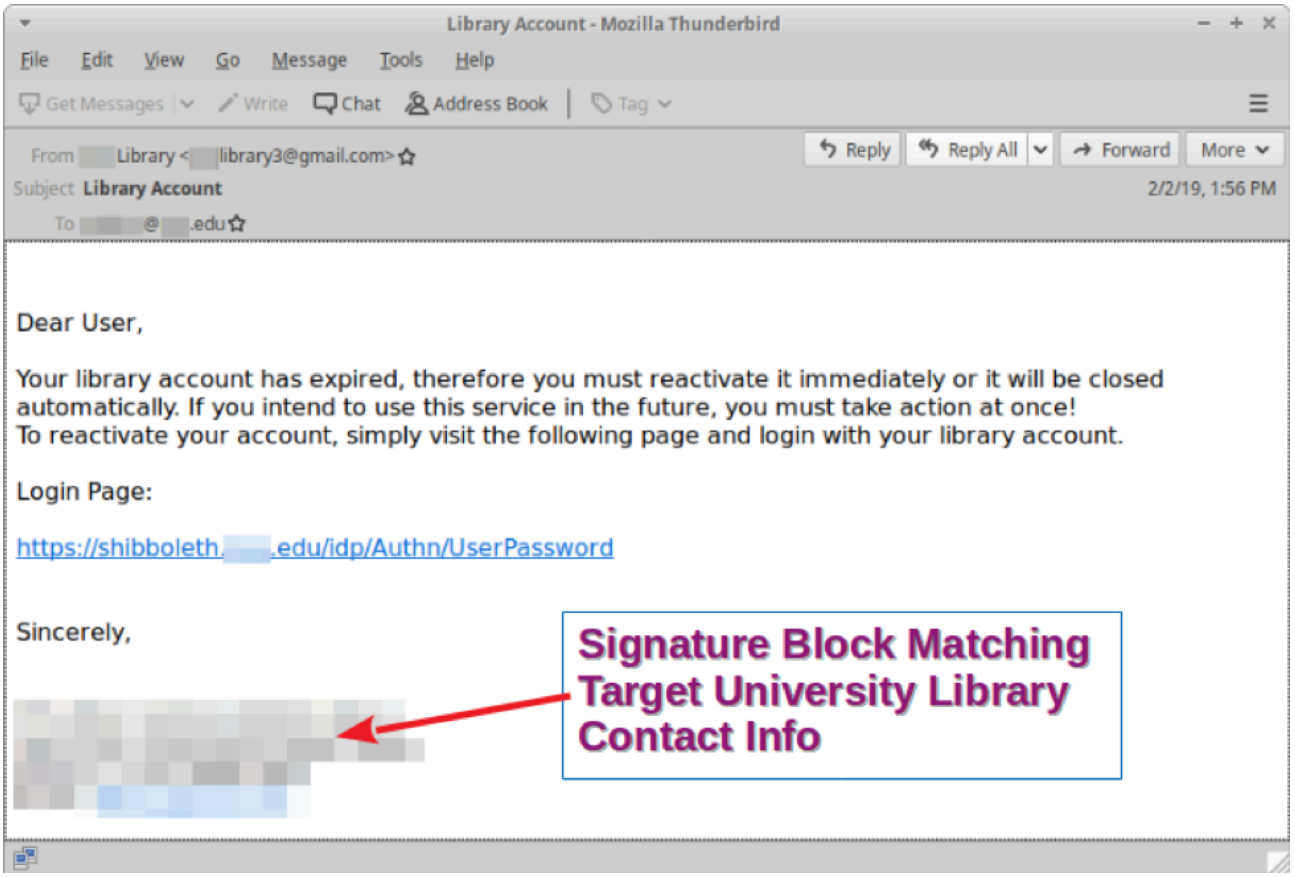

Figure 6: Silent Librarian message with spoofed sender address and fake signature block

The URLs in these messages link to cloned university login portals that use stolen branding and lookalike domains to manipulate recipients into disclosing their login credentials. After submitting credentials, victims are often redirected to the actual university library login page, leaving no indication that their information had just been phished.

The group is also known for leveraging local events and alerts to add legitimacy to their lures and time attacks to periods during which security and IT staffing may be minimal as shown in Figure 8.

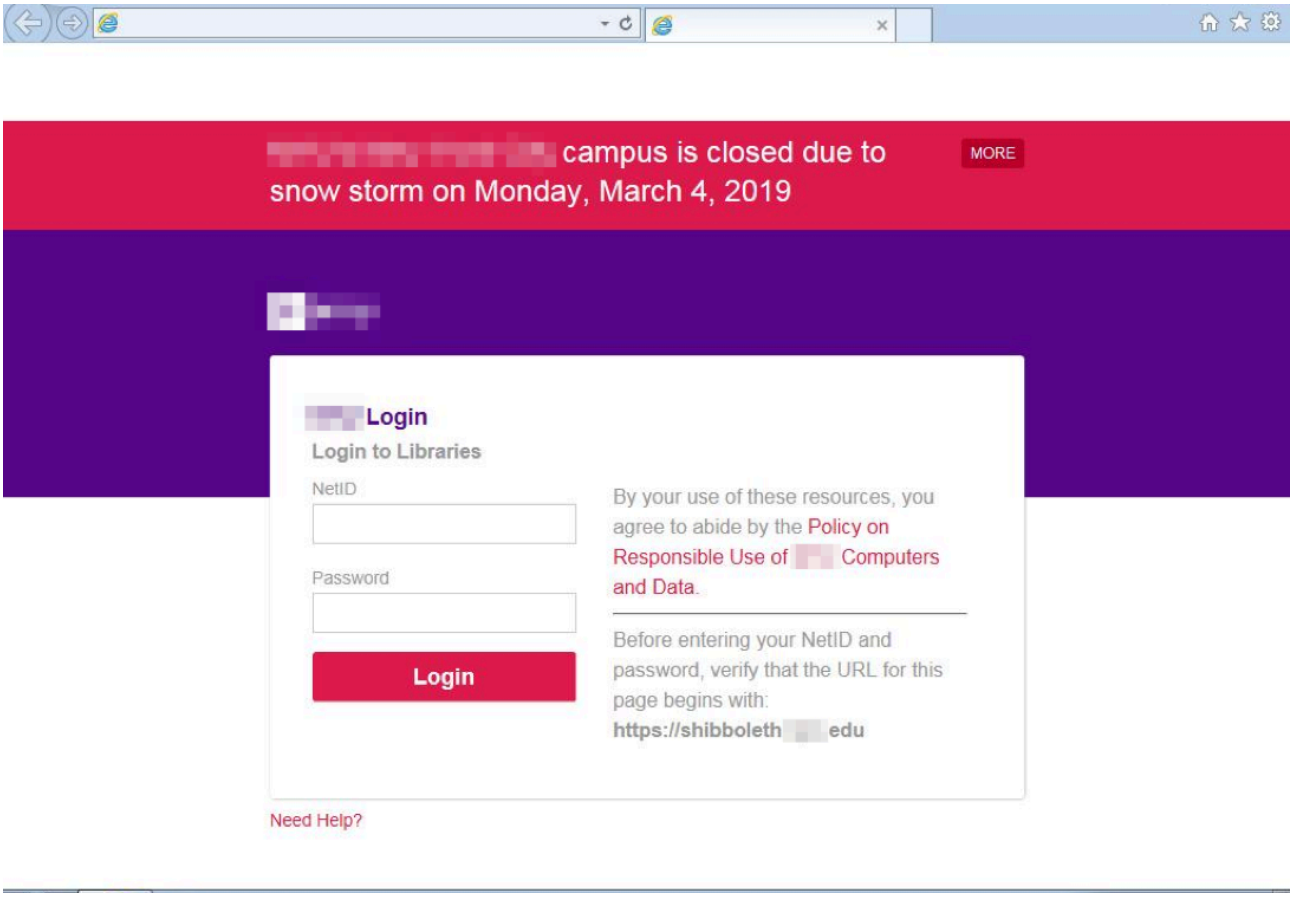

Figure 7: Fake university login portal with spoofed display name, stolen branding, and accurate weather forecast warning

Conclusion

Phishing is one of the most prevalent types of threats that Proofpoint observes. Collectively, phishing campaigns account for millions of messages per year. Threat actors use stolen branding and other social engineering mechanisms to manipulate victims into disclosing personal data or login credentials. Phished credentials often serve as the foundation for business email compromise, which is difficult to detect because affected accounts are legitimate.

TA407/Silent Librarian has proved to be a notable threat in the phishing landscape, using low volume, highly targeted, socially engineered campaigns to steal students' login credentials. These campaigns affect hundreds of universities in the US.

Significantly, recent Proofpoint research revealed that the education sector is particularly vulnerable to attacks on cloud services with the highest success rates for unauthorized login attempts of any industry. This demonstrates the value of stolen credentials to threat actors and the broad attack surface inherent in university environments.

As a recommendation to mitigate these risks, we advise universities to:

- Implement comprehensive antivirus/anti-phishing services
- Instruct students on how to recognize malicious emails

- Implement multi-factor authentication (MFA) in university email systems, client devices, and application portals
- Advise their students and faculty on how to:
    - Recognize malicious emails that often rely on similar social engineering techniques
    - Avoid emails that contain typical indications of malicious intent:
        - Spelling mistakes
        - Grammatical issues
        - Unsolicited requests for information
        - Suspicious links that may spoof reputable domains
    - Report suspected malicious emails to the university IT department
    - Avoid interacting with suspicious messages, especially ones that request personal information or prompt the student to log in to a university service
    - Be aware of potential phishing attacks when threat actors, including TA407, are most active:
        - September-November (Beginning of school year)
        - January-February (return from winter break)
        - April-June (conclusion of the school year)

References

[1]https://www.proofpoint.com/us/threat-insight/post/proofpoint-releases-q4-2018-threat-report-and-year-review

---