

Phishing Without a Rod

2020 Internship Showcase

Daniel Malloy

High Point University

internships@rti.org





Security Software Experience

- ArcSight[®] ESM
- Tenable[®]
- Tenable.IO[™]
- FireEye
- McAfee[®] Security Suite



Spotting Phishing Emails

[Attention] - Rti server request #4zl8g

RS Rti Support <greg@parkwayservices.com>
To [REDACTED]

← Email clearly not from Microsoft or RTI

Reply Reply All Forward ...

Tue 7/21/2020 12:41 PM

i This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

EXTERNAL: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. ← Always a red flag

Office 365

Dear [REDACTED]

Office 365 has prevnated the delivery of 3 new messages

← Obvious spelling mistakes

to your inbox as of Tuesday, July 21, 2020 9:41:27 AM (UTC).

You can review these here and choose what happens to them.

[Review](#)

Thanks ← Informal sign-off with no formal footer

Screenshot taken from Microsoft Outlook and censored to protect employee's identity.



It Does Not Hurt to Double Check

This is the supposed "Microsoft" link.

404 indicates an offline site.

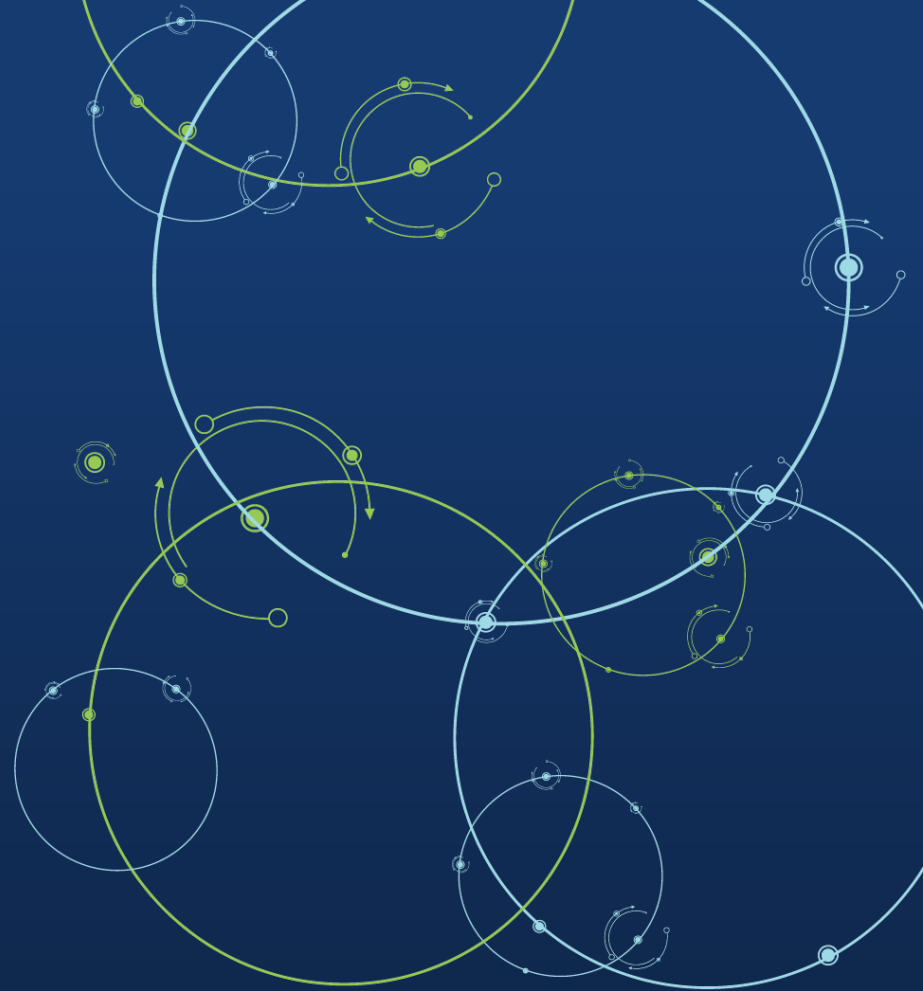
The screenshot shows the VirusTotal interface for the URL `http://4zl8g.ifhelum.xyz/@40@14@/`. The status is "404 Status", indicating an offline site. The content type is "text/html; charset=iso-8859-1" and the timestamp is "2020-07-23 17:32:17 UTC a moment ago". The interface also shows a "Community Score" of 0/79 and a message "No engines detected this URL".

404	text/html; charset=iso-8859-1	2020-07-23 17:32:17 UTC
Status	Content Type	a moment ago

Screenshot taken from [virustotal.com](https://www.virustotal.com), a free and public security tool.

Acknowledgments

I would like to thank my mentor, Austin Chang, and my manager, Sotorn Muangmanee, for guiding and advising me these past few weeks, as well as the rest of the Security Team and the entire Global Technology Solutions Team.





Thank you

Contact: Daniel Malloy | email: internships@rti.org