Phishing Without a Rod

2020 Internship Showcase

Daniel Malloy

High Point University

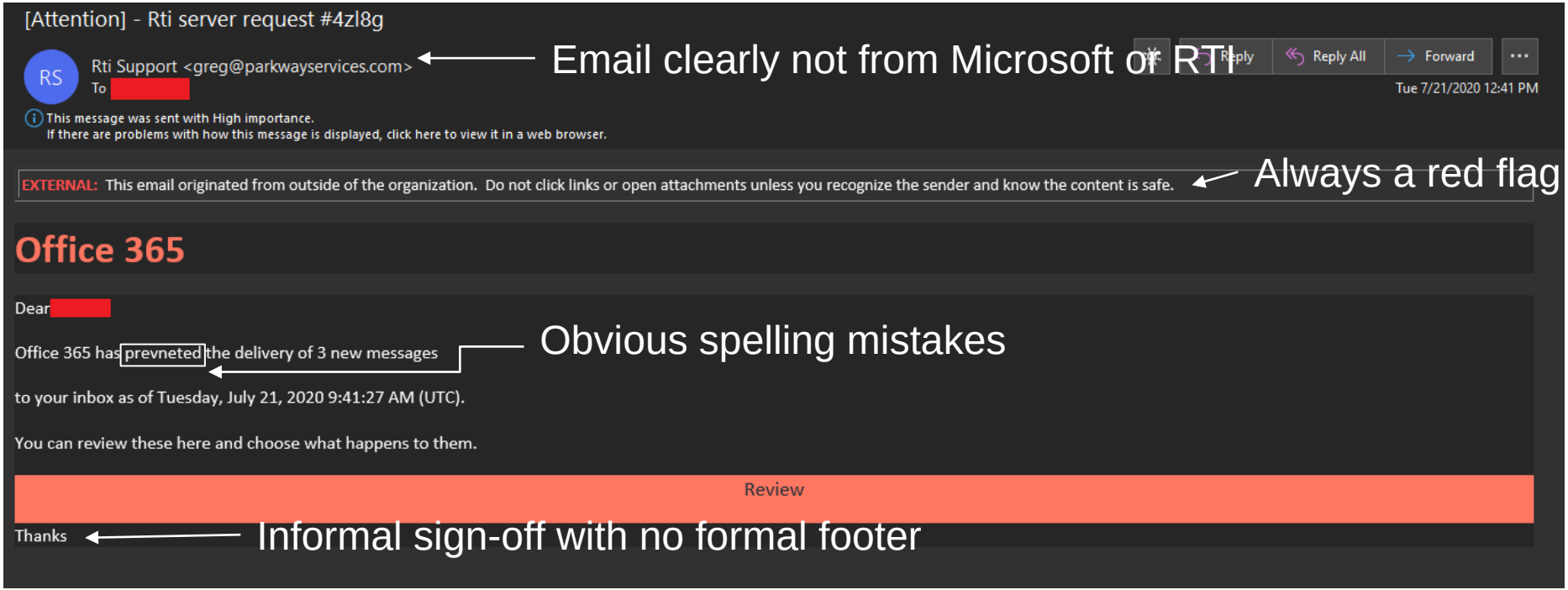
internships@rti.org

RTI INTERNATIONAL

Security Software Experience

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

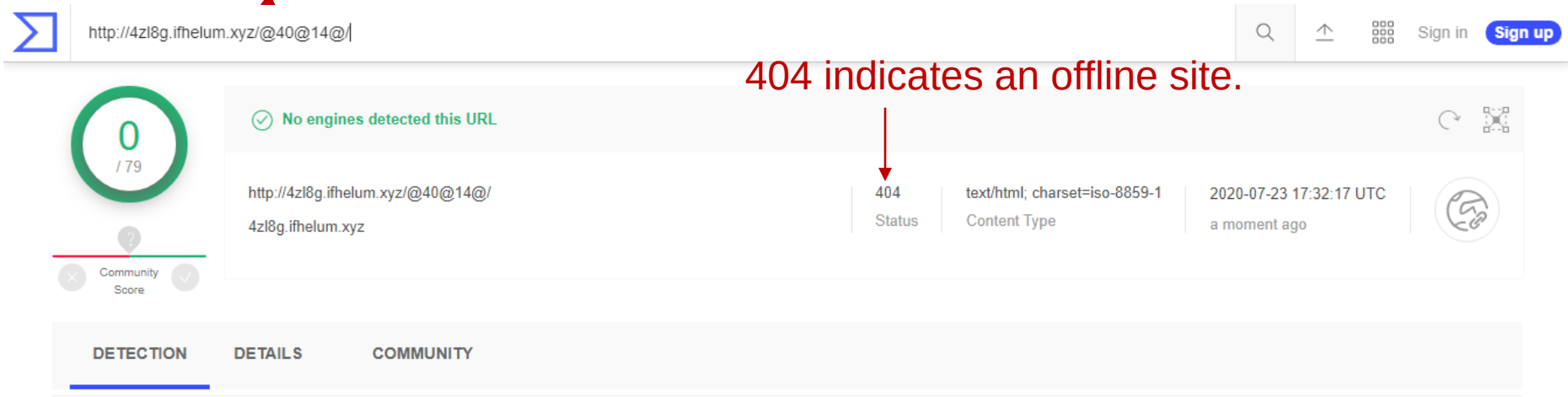
Spotting Phishing Emails



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.



Screenshot taken from virustotal.com, a free and public security tool.

When All Else Fails, There Are Headers

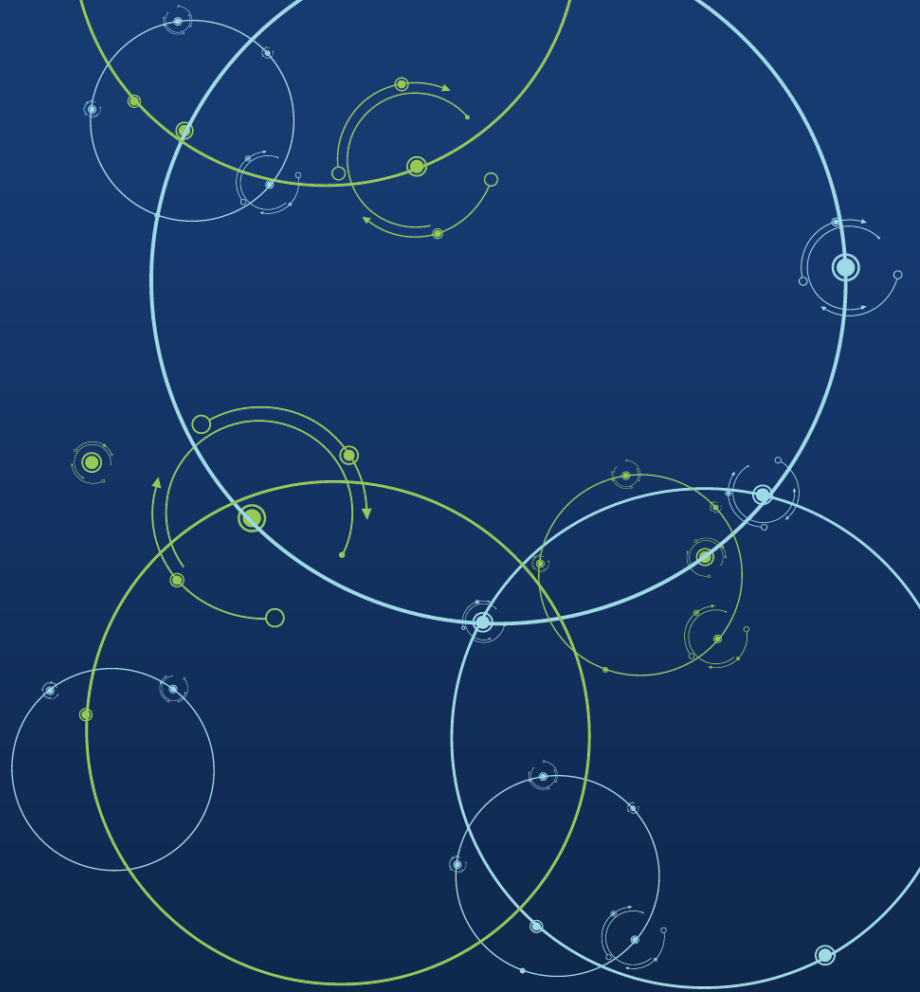
X-Ms-Exchange-Transport-Crosstenantheadersstamped	MN2PR07MB7277
X-Fe-Etp-Metadata	eyAidGlkIjogIjVEQkMwODU5MEE0OEI2MUY1M2ZkMTliN2IiLCAiYWNjZXB0ZWRfdGltZXN0YW1w IjogIjIwMjAwNzIxMDk0MTMwIiwgImFjY2VwdGVkX3RpbWVzdGFtcF9lcG9jaCI6ICIxNTk1MzI0 NDkwIiwgImRvbWFpbl9uYW1lIjogInJ0aS5vcmciLCAiYXR0X2NvdW50IjogLTIsICJzcmNfaXAi OiAiMTA0LjQ3LjQ0LjUxIiB9
X-Fe-Etp-Advanced-Analysis-Result	Clean
Message-Id	<1MbjBo-1kXQVd3Exa-00dFxw@mrelayeu.kundenserver.de>
X-Ms-Exchange-Organization-Expirationstarttime	21 Jul 2020 09:41:35.5696 (UTC)
X-Ms-Exchange-Organization-Expirationstarttimereason	OriginalSubmit

The original email was shown as greg@parkwayservices.com.

Screenshot taken from mxtoolbox.com, a free and public security suite.

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