Michael Esposito

Network Defense 2

Spearphishing Example

My spearphishing campaign targets users of the payment service Venmo. The campaign targets students, and Venmo is popular among students in DC and Foggy Bottom. It is possible to extract the entire directory of student email addresses from the following website: <https://my.gwu.edu/mod/directory/index.cfm>. Two letters are required to search, but going alphabetically (aa, ab, ac, ad…) one could assemble a very large list of target emails at the GWU community. A subset of this community may have Venmo registered to a @gwu.edu email address, making this spearphishing campaign valuable. GW’s student directory can reveal each target’s first name. This information can then be integrated into an email stating that their account was logged in from an unidentified device. This email will ask that the target log in to confirm if this was or was not an authorized account access.

I chose to use Venmo as the vehicle for my phishing campaign because I know its use is widespread among students. Many people also provide their Venmo account direct access into their bank account, making unknown account access a fairly serious concern. I provide a link in my email to a website where the user should login to review the completely made-up unauthorized account access. Hopefully, a few users would then enter login credentials into this form. These credentials could then be used to login to victims’ Venmo accounts, bank accounts, email accounts or anything else valuable.

The HTML formatting for my email was generated by an actual Venmo email. I slightly modified the code, which can be seen below. A screenshot of the email in Gmail’s web client is also included below.

1. <div style="margin:0">
3. <div style="font-family:'helvetica neue'">
4. <div style="margin:0 auto;max-width:380px;font-size:16px;line-height:24px">
5. <div style="padding:24px 0 20px;text-align:center;background-color:#3c95d2">
6. <img src="https://ci5.googleusercontent.com/proxy/u9iMZvFSOSqmGnx9r8JJ\_zM2dXee-TSu8T9n6hDWbUTUbtdXONoTBmuzcGhrRe8jEJnoc6csJLgsSRxmxDX3pazx3aAZNXSU4lkFdg=s0-d-e1-ft#https://s3.amazonaws.com/venmo/venmo-logo-white-2x.png" alt="venmo" title="venmo" style="width:105px;height:20px;display:block;margin:0 auto" height="20" width="105" **class**="CToWUd">
7. </div>

10. <div style="padding:36px 24px;margin-bottom:40px;background-color:#fff;border:1px solid #d9d9d9;border-top:0px">

13. <div>
14. Hi Michael, <br>
15. <br>
16. We noticed an attempt to sign in to your account from a **new** device or browser.
17. <br><br>
18. If **this** wasn’t you, please immediately login and reset your password. You can **do** **this** <a href="https://goo.gl/Apnp9Z" target="\_blank">here</a> or on the sign-in screen in the mobile app.
19. <br><br>
20. You can manage your remembered devices from your <span **class**="il">Venmo</span> settings. If you have questions or need help, please visit our help center or contact us by replying to **this** email.
21. <br><br>
22. Thanks,<br>
23. Team <span **class**="il">Venmo</span>
24. </div>
26. <img src="https://ci3.googleusercontent.com/proxy/O8GnLqH\_xjeg3\_\_1LHS3rC3687N3RCotVdTS6oeQ5iLv3uG3qi86y5Q3fSbT260qscOYvih2aB0rm3lLSsl5c4jwvOrvZfcPV1Vm115CQg=s0-d-e1-ft#https://venmo.com/vt.png?scat=tfa\_login\_attempt&u=3256865" **class**="CToWUd">

29. </div>
30. <div style="font-size:11px;line-height:20px;color:#bfbfbf;text-align:center;max-width:380px">
32. <div style="margin-top:5px">PayPal is located at 2211 North First Street, San Jose, CA 95131</div>
33. <div style="margin-top:10px;font-size:11px">


37. </div>
38. </div>
39. </div>
41. <div><img src="https://ci3.googleusercontent.com/proxy/O8GnLqH\_xjeg3\_\_1LHS3rC3687N3RCotVdTS6oeQ5iLv3uG3qi86y5Q3fSbT260qscOYvih2aB0rm3lLSsl5c4jwvOrvZfcPV1Vm115CQg=s0-d-e1-ft#https://venmo.com/vt.png?scat=tfa\_login\_attempt&u=3256865" **class**="CToWUd"></div><div **class**="yj6qo"></div><div **class**="adL">
43. </div></div><div **class**="adL">
44. </div></div>

