PHISHING FOR PASSWORDS

Graduate Project 2: Policies, Procedures and Practices

Eliora Horst

COMP 448: Network Security

Mr. Corby Schmitz

Loyola University Chicago

Policy I: Password Security

Password Standards for Fictional Company LLC

Objective

Passwords are one of the first walls of defense when it comes to accessing protected data and systems. All employees and associates of Fictional Company LLC are required to maintain a secure password according to the guidelines detailed below, as well as make any appropriate changes to their passwords following any updates or revisions to this policy.

Scope

This standard is inclusive of all employees and associates of Fictional Company LLC who must have access to the company network as part of their employment, via company issued desktop and laptop computers, as well as mobile devices.

Standards

Network Password Management: The following details the requirements of any standard level password.

- Passwords must have a minimum of 10 characters and a maximum of 18. While longer passwords are more difficult to remember they are more secure, so the use of a password manager is encouraged. See below for the policy on password managers.
- Passwords must contain a combination of uppercase and lowercase characters, and at least one number. It is encouraged not to simply replace letters with similar looking numbers.
- Passwords must contain one special character. It is encouraged not to simply add an exclamation point (!) to the end of your password to satisfy this requirement.
- Passwords must be unique. Any passwords that are part of the list of most common passwords list (See Appendix A: Common Password List) will not be accepted.
- Passwords are no longer set to expire, but the Information and Technology Department reserves the right to instantiate a password change if the need arises.

Six unsuccessful attempts in network, and three unsuccessful attempts via remote access are allowed before an account is locked. You must contact the IT Department immediately to regain access to your account.

Password Security:

- Passwords shall not be written or maintained in any text format.
- The IT Department encourages the use of a password manager to maintain all company passwords and approves the use of 1Password.
- Passwords shall not be shared between employees.

Remote Access:

Remote access to the Fictional Company LLC network will only be approved from company provided devices. Personal computers and mobile devices are prohibited from accessing the network unless given special permission from the IT Department. Remote users must use multifactor authentication to access the company network. Remote users must also submit proof of anti-virus software on their machines.

Password Change:

As stated above, passwords will no longer be required to change according to a specific time limit. Users may change their password according to their own discretion or the discretion of their supervisors, but no more than three times a month, and all requests for password change must be approved by the IT Department. Forgotten passwords cannot be recovered, so if a user forgets a password, it must be reset.

Version 1.0

Policy II: Phishing

Phishing policy for Fictional Company LLC

Objective

Phishing is a type of threat where a malicious party poses as a trusted entity to get the user to share sensitive information. While Fictional Company LLC uses cloud-based email protection and anti-spam filters, employees must be prepared to address a phishing attempt if one should occur. All employees at Fictional Company LLC must familiarize themselves with the tactics used by such attackers and know how to respond.

Scope

This policy is inclusive of all employees and associates of Fictional Company LLC who have been issued a company email and use it for internal and external communication, and employees who have received a company issued mobile device or have their personal mobile device associated with their employment.

Standards

Interacting with Email: For the purposes of this policy, interaction with email includes:

- Providing information via written text or embedded images
- Attaching files of any kind
- Clicking on embedded links

Identifying Malicious Emails:

The following is the standard by which to determine if an email may not be from a trusted source. If you have any doubts, always consult your supervisor or the IT department before any interaction.

- Investigate the sender
    - Does the email appear to not be from another Fictional Company LLC employee, or an already established contact?
    - Is the name of the sender misspelled?
    - Is the email domain a random string of characters and numbers?
- Any email that does not have the Fictional Company LLC as the domain name, or is part of our list of trusted connections, must be verified by our IT department.
    - Any email from a non-commercial/business domain (google, outlook, yahoo, etc.) should be considered untrustworthy until proven otherwise.
- All emails sent within the Fictional Company LLC network are authenticated – non-authenticated emails are not to be trusted until approved by the IT department.
- Investigate the body of the email
    - Are there lots of links that appear as text or buttons?

- Is the body of the email an image instead of plain text?

If you identify one or more of these concerns with an email, do not interact with until you have reported it to the IT department and received approval that it is a safe and valid email.

Employee Responsibilities:

The following is a guideline for employees to follow when using email in the Fictional Company LLC network.

- Do not click on any links contained in an email without verifying where it will go. Any link that is deemed suspicious by our security system will give a warning to the user and to the System Administrator before redirecting the user.
- If an email requests that you visit a trusted website, type that website into the URL bar and do no use any provided links.
- Report any suspicious email activity as soon as you become aware of it. Do not attempt to interact with the email.

Version 1.0

Appendix A: Common Password List

Below is list of common passwords that shall not be valid for any users of the Fictional Company LLC network. This list continues to be amended and expanded.

1. 123456
2. 123456789
3. Qwerty/qwerty
4. Password/password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. 123456789
14. DEFAULT
15. 0
16. abc123/Abc123
17. 654321
18. 123321
19. Qwertyuiop
20. Iloveyou
21. 666666
22. password1

Works Cited

Ave, INFORMATION TECHNOLOGY SERVICES · 1032 W. Sheridan, Chicago, and Disclaimer 2022 · Privacy Policy. "Password Standards: Information Technology Services: Loyola University Chicago." Accessed April 1, 2022. https://www.luc.edu/its/aboutits/itspoliciesguidelines/password_standards.shtml.

Colby, Clifford. "The Best Password Managers for 2022 and How to Use Them." CNET. Accessed April 1, 2022. https://www.cnet.com/tech/services-and-software/best-password-manager/.

SHRM. "Computer Passwords Policy," July 7, 2021. https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/passwordpolicy.aspx.

Jr, Tom Huddleston. "These Are the 20 Most Common Passwords Leaked on the Dark Web — Make Sure None of Them Are Yours." CNBC, February 27, 2022. https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html.

Auth0 - Blog. "NIST Password Guidelines and Best Practices for 2020." Accessed April 1, 2022. https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/.

SearchSecurity. "Phishing Protection: Keep Employees from Getting Hooked." Accessed April 1, 2022. https://www.techtarget.com/searchsecurity/feature/How-to-avoid-phishing-hooks-A-checklist-for-your-end-users.

sarah.henderson@nist.gov. "The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails." Text. NIST, September 17, 2020. https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click.

"Time for Password Expiration to Die." Accessed April 1, 2022. https://www.sans.org/blog/time-for-password-expiration-to-die/.

"What Are The Most Common Passwords of 2021?" Accessed April 1, 2022. https://www.schneiderdowns.com/our-thoughts-on/most-common-passwords-of-2021.