Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

A Strategy to Get Started with an Information Security Program

Best Practices for Passwords and Account Security

Patrick Rost prost@dopkins.com

Published June 23, 2021 - In our previous blog on the cost of a data breach, we discussed that compromised credentials are both the most frequent and most costly threat vector for organizations, stressing the need for secure passwords. Most times a password is the ONLY protection for your data. This blog will take a look at the best practices around passwords and account security including things you should and should not be doing.

How do accounts become compromised?

There are several ways a user's password can become compromised. Below are a few of the most common:

- **Phishing attack**
  - In a phishing attack, employees could be tricked into entering their password on a malicious site. In our previous blog covering Cybersecurity Awareness Training, we discussed phishing and how training employees can make them less vulnerable to this type of attack.
- **Exposed in previous breach**
  - The goal of many attacks is to steal credentials so they can be used to access other accounts. Attackers will try stolen username/password combinations against many different sites in the hopes to gain access, in what is known as **Credential Stuffing**.
- **Easily guessed**
  - Attackers will attempt **Password Spraying**, which is using lists of commonly used passwords, to gain access.
  - Based on research by NordPass (https://nordpass.com/most-common-passwords-list/) the ten most used passwords of 2020 were: 123456, 123456789, picture1, password, 12345678, 111111, 123123, 12345, 1234567890, senha (Portuguese for password).
    - 8/10 of these have been used over 2 million times and can be cracked in less than a second.
    - 5/10 were on the top ten from 2019.
- **Brute Force**
  - Attackers will use programs to keep guessing using every combination of characters.
  - This method is more difficult than the previous three because it usually takes more time, technical expertise and can be expensive.

Ways to prevent compromise

- **Use long passwords**
  - Minimum of 12 characters, but 16+ is best.
  - 8-character passwords can be cracked in about 3.5 hours, 12 characters take about 177 years, 16 characters take over 81 million years.
  - Protects against Brute Force attacks.
- **Use Passphrases, not passwords**
  - Could be from a past memory that only you would know. Things that are funny are easier to remember.
  - Examples:
    - I'm dreaming of a white Christmas [33 characters with spaces]
    - From the Halls of Montezuma [27 characters with spaces]
  - Easier to remember than typical (and short) complex password like: uX76$!6wcZ
  - Protects against Password Spraying, additional protection against Brute Force attacks.
- **Use sequence of four or more random and unrelated words.**
  - Do not use anything that is public knowledge or easily guessable (especially pet or children names)
  - Examples:
    - posing granular repulsion crown [31 characters with spaces]
    - negative trombone goon serpent [30 characters with spaces]
  - Easier to remember than typical (and short) complex password like: uX76$!6wcZ
  - Protects against Password Spraying, additional protection against Brute Force attacks.
- **Do not re-use passwords**
  - Visit the site www.haveibeenpwned.com to see if your email or phone number are linked to a data breach.
    - Exposed passwords will be used to access your other accounts. Immediately change the password for any account that has been exposed.
  - Protects against Credential Stuffing.
- **Do not store passwords on your computer, within your email/contacts, or on hand-written notes near (or especially attached to) your PC.**
  - If your PC or email account is compromised the file can be stolen and all your accounts are at risk.
  - Notes at your computer allow anybody to walk up and sign in to your accounts.
  - Hand-written passwords should be locked in a secure place.

Additional Recommendations

- **Use a credential manager**
  - Not the same as saving in your web browser, which can also be stolen.
  - Will store long passwords so you do not have to memorize them. This allows each account to be unique so there is no re-use.
  - Most have password generators so they are truly random.
  - This account is secured by one long passphrase and multi-factor authentication.

- **Enable Multi-Factor Authentication (MFA)**
    - Uses more than one of the following factors to authenticate:
        - Something you KNOW (passphrase, PIN)
        - Something you HAVE (security token, bank card)
        - Something you ARE (biometrics: fingerprint, retina scan)
    - Should be enabled on all accounts that offer the option.
    - Frequently used:
        - Text/email code
        - Authenticator app
        - Physical authenticator/token
    - **Does not eliminate need for good passwords**.
- **Account recovery questions**
    - **DO NOT** use them as intended.
        - Most are guessable, especially with the amount of information shared or compromised on the internet.
    - Create unrelated passphrase or long generated password for each question.
        - Store these in your credential manager.
    - Make up answers that are not accurate which are not easily guessable or publicly known.
        - Pet: Rover
        - School: Hard Knocks
- **Remove phone number as recovery method**
    - Phone numbers are not secure and can be simulated.
    - Old number stays attached to accounts if you get a new one.
    - Rely on your strong passphrases and use of credential manager.

If you would like to have a conversation and discuss how to implement account security controls contact Patrick Rost (prost@dopkins.com). Check out our STARTegy page for more information about our Strategy for Getting Started with Information Security.

Links in article

- -
- -
- -