Milima
Security

Strong passwords and Multi-factor Authentication

In technology, a password(also known as credential) is a string of characters that allows access to a computer system or service. Passwords are one of the primary targets of cyber attackers, especially highly skilled ones and those attempting to persist long-term in a target organization's environment. Passwords are simple and yet can be a confusing security behavior for people and yet passwords are also often one of the greatest risks to most organizations. Recent reports show that attackers have shifted focus from malware to passwords.

Numerous phishing and social engineering attacks were previously used to attack and infect systems but now they have become the means to gain valid passwords. Cyber criminals now know that it is harder for security teams to detect an intruder who is using valid credentials to access an organization's data.

The term is called '*living off the land*' and implies a cyber attacker is using the same valid tools and credentials that authorized individuals use, so the cyber attacker's activities blend in with and appear to be legitimate. This is why passwords have become one of the primary targets and why stolen or compromised credentials have become one of the top risks for organizations.

Key recommended lessons about passwords for your focus.

Your objective for password training should be making passwords as simple as possible. Considering the numerous changes over the recent years on best practices for passwords like password complexity being replaced with password length. One of the most effective ways to simplify passwords in your organization could begin with a review and update of your organization's security policies and procedures concerning passwords.

1. **Unique**: Emphasize and train on the importance of each and every account (both work and personal) having a unique password for that account. This ensures that if one account is compromised, all other accounts are still secure.
2. **Passphrases**: Replace password complexity with password length whenever possible, teach people the concept of passphrases. Passphrases can be sentences or a series of random words that create long passwords that are both easier to remember and type.

3. **Local language**: The internet is mostly written in English, teach people to consider using one of their local/ second languages to create unique strong passwords.
4. **Password Managers**: If possible, encourage the use of password managers. Managing a long, unique password for each account is difficult for people, as many people can have over 100 passwords. The simpler we make a behavior, the more likely people will exhibit it. If your organization prohibits the use of password managers, keep in mind that people will still likely write their passwords down or use something like Google Docs or spreadsheets to manage all of their passwords.
5. **MFA**: Whenever possible, people should enable Multi-factor Authentication (commonly called Two-Factor Authentication or Two-Step Verification) for their work and personal accounts.

Strong, secure passwords are key to helping reduce risk to your organization and for people to protect themselves at home. However, in the past, security policies have traditionally made passwords both confusing and difficult. The simpler we can make strong passwords for people, the more likely they will use them, and the more we all benefit.