Haekka

Lesson 5 | Securing Your Accounts

Updated 2020-09-14

Given the massive changes in how and where work is being done, the security best practices and priorities need a refresh. One of the big challenges facing security groups is securing cloud and SaaS services. The number of software services, the low cost of those services, and the ability of end-users to deploy and manage new services directly compound the problem. It is not uncommon for employees to have to use 10+ or even 20+ different software applications today, software applications that are often owned and managed by different groups.

Below are the best practice considerations for securing your accounts and your identity online. These apply to both personal and company software and accounts. You should review your company policies and procedures to ensure alignment with these practices.

- **Identity**. Securing identities across multiple SaaS services is a challenge. One easy way to help solve this is by using a single sign-on solution like Okta. This unifies identity management and is the easiest way to standardize managing identities across multiple SaaS apps.
- **Passwords**. Passwords in 2020 are an inherently necessary but weak form of protecting accounts. Passwords reuse across both corporate and personal accounts is problematic due to widely available databases of breached passwords; attacks that test 1000s or even millions of breached passwords are called *credential stuffing*. Some new applications forego the use of passwords in place of secure, dynamic, unique links. Nevertheless, passwords are still here. Some best practice rules are to use long passwords (over 8 characters), do not use easy to guess or dictionary words, and do not reuse passwords.
- **Password manager**. Password managers are a good and secure way to store complex passwords across multiple services. Password managers can also generate long, strong passwords for you. Make sure that you control access to your password manager. Good examples are 1Password and LastPass.
- **Multi-factor authentication (MFA)**. MFA requires multiple forms of verification (not just username and password) before granting access to systems. There are multiple methods to implement MFA including phone / SMS, authenticator apps, and token-based applications. Whatever the method, using MFA reduces the chance of account compromise by over 99%. Duo is a provider of MFA solutions for businesses.
- **Access requests**. There should be an established process to request and grant access to applications. Each application should have an owner - either a group or individual -

that has to explicitly grant access to SaaS services. Each one of these access requests should be formally documented.

With identities increasingly online, attacking them has become a lot easier. And attacks can be launched at scale. Gaining access to your software accounts often leads to additional attacks.

Set strong, unique passwords, and make sure you use multi-factor authentication (MFA).