

Staying Safe Online

Jeff Howe, Senior EA Architect 10/28/16

Every day it seems there are new reports of cybersecurity breaches and online account thefts. October is National Cybersecurity month and along with this event comes numerous articles on how to remain safe online. Below are a few practices that can help protect online accounts from being compromised by attackers.

Password managers have become an essential tool to help create strong passwords and manage access to online accounts. Key features include browser and mobile app integration to allow automatic capture of login details and the ability to automatically login. Multiple device and platform support can allow management and access to login details from all connected devices.

Another safeguard promoted by cybersecurity experts is enablement of multi-factor authentication. This process typically involves designating a secondary email address or device which receives a notification with a code that must be entered before a password reset is permitted. Enabling multi-factor authentication where supported can reduce the risk of an attacker gaining access and taking control of online accounts.

On mobile devices, security features should be enabled which require additional authentication before changes can be made to device settings. Do not use the same password or passcode which provides access to the device itself. Enable features which automatically lock devices after a specified time period in order to reduce the likelihood your device is compromised without your knowledge.

Security questions used to authenticate a password reset are another area of concern. Such questions are thought to provide information that only the account holder would know. Answers to questions such as, "What city were you born in" or "What is your oldest sibling's first name," can be discovered through internet searches or by reviewing social media profiles. Using the same thought process as with passwords, provide password-like answers rather than the actual answers. Use a password manager to store the questions and answers.

Reviewing passwords and enabling additional security features is time consuming. However, consider the time spent in preparing a strong defense worthwhile when compared to the time spent recovering from an attack which compromises online accounts.