



Issued 6/29/18

Scammers are Controlling Apple Accounts using a Feature for Families to Share Apps

Scammers in China are hijacking people's Apple IDs and making purchases via an iPhone and Mac feature called "Family Sharing." The feature is designed to help families share apps and music, but the scammers are using it to lock out the actual owner of the account and buy in-app purchases and iTunes gift cards. When David tried to download apps on his iPhone and iPad recently, he found he wasn't able to because his account was linked to something called "Family Sharing." That's a feature that Apple introduced in 2014 to make it easier to share apps, iCloud storage, and iTunes content like music and movies with up to five family members. But this was news to David, who says he didn't remember turning on Family Sharing. After he dug into his account settings, he received a popup that to remove himself from the Family Sharing account he needed to contact a name that was in Chinese — and he had no way to get in touch. There are a handful of posts on Apple's support forums and Reddit that detail similar stories of accounts that couldn't buy apps or in-app purchases due to issues involving the feature. Apple ID usernames and passwords can be an attractive target for scammers, who sometimes use Apple's security features to lock the data on an attacked device and ask for ransom. When setting up Family Sharing, the user being added receives an email or text with an option to join or decline, according to Apple. It's possible that many of these people who have reported the problem may have received the notification and mistakenly approved it, although most of the reports online say they believe that didn't happen. There's another way to add an account to Family Sharing: if the administrator of the family has your password. This is

useful for parents and other legitimate Family Sharing users. But that also means that an attacker could obtain someone's password, perhaps through a fake phishing email or one of the leaked databases out there, and then use that password to take over the Apple ID account. But if an attacker had your Apple ID and password, which means could gain access to your account directly if two-factor is not turned on. So it's still unclear why the Family Sharing feature is entering into this phenomenon — why would a scammer make purchases with a linked account instead of the original?