Dubious security vulnerability: Accessing information across accounts after changing email address

devblogs.microsoft.com/oldnewthing/20211213-00

December 13, 2021

Raymond Chen

A security vulnerability arrived which basically went like this:

- Person 1 creates an account.
- Person 1 links the account to a Microsoft Account.
- Person 1 creates some files and saves them to the Documents folder.
- Person 1 uses *Remember my password* to remember passwords for a variety of locations.
- Person 1 agrees to sell the PC to their brand-new best friend, Person 2.
- Person 1 and Person 2 meet to arrange the purchase.
- With both people present, Person 1 signs in, unlinks the Microsoft account, opens the *Change Password* page, and enters the old password.
- Person 2 enters the new password and links the account to Person 2's Microsoft Account.
- Person 2 takes the PC home and finds that they can access the files in the Documents folder, even though they belong to Person 1. They can also sign into various sites using Person 1's saved passwords.

This was reported as a security vulnerability because Person 2 shouldn't be able to access Person 1's files or see Person 1's saved passwords. Person 1's password is no longer valid, and their Microsoft Account is no longer linked. The account now belongs to Person 2.

Well, the thing is, as far as the system is concerned, Person 2 and Person 1 are the same person!

The scenario above is equivalent to

- Person 1 creates an account.
- Person 1 links the account to a Microsoft Account.
- Person 1 creates some files and saves them to the Documents folder.
- Person 1 uses *Remember my password* to remember passwords for a variety of locations.

- Person 1 decides that they want their primary association to be with a different Microsoft account, so they unlink the old Microsoft account, change their password, and link to a new Microsoft Account.

In this case, Person 1 expects to be able to retain access to the files in the Documents folder still use saved passwords to sign into various locations.

The security error occurred when Person 1 went through half of the password reset sequence and let Person 2 complete the process. By typing in the old password and then handing over the machine, they effectively *gave away access to their account*. When you do that, you let anybody act as if they were you! And that includes identity theft.

It's like you have a membership at a club. You decide to sell the membership to somebody else, but instead of arranging it through the club membership office, you go to the web site and change the credit card number, and then go through the PIN reset page together, where you type your old PIN and the other person types the new PIN, and once that's all done, you give them your membership card. Maybe to make things look good, you replace the name and photo on the membership card. The second person goes to the club membership office, swipes the membership card through the machine, and all of your membership history shows up. Information disclosure to another person!

No, as far as the membership system is concerned, that's still *your* membership card. You changed the credit card that's used to pay for the membership, and you changed the picture and name on the card, but what the membership system cares about is the member number that's embedded in the chip on the membership card, and the fact that the person in possession knows the PIN. As far as the membership system is concerned, that person holding the card *is still you*.

What Windows cares about is the user SID, which is embedded in the account you signed in with. And so far, Person 1 hasn't changed the Windows account. They changed all of the account's superficial attributes: The name and picture on the login screen, the password, the associated Microsoft Account, but is still the same account with the same SID. And therefore, it still can access anything that the SID has access to, which includes all of Person 1's old documents.

If you don't want somebody else to be able to access your stuff, then don't give them the ability to impersonate you by handing over your password. If you want to set up a new account, set up a new account; don't reuse an old one. And if you want to sell your PC to somebody else, you should reset it properly.

Raymond Chen

Follow