5 Reasons We're Terrible at Choosing Passwords

Psychology explains why we fail, even though our security depends on it.

Posted Oct 08, 2014

Source: Tab62/Shutterstock

Why do we consistently fail to choose safe passwords? Here are 5 reasons, explained by cognitive psychology:

1. We pick easy-to-guess passwords.

   It is simply hard to remember a completely random string of 8 characters with uppercase letters, lowercase letters, numbers, and special characters. A name or date (which are among the most common, and least secure, choices) is far easier to remember, reducing how hard we have to work every time we log in. In other words, our memory limits lead us to choose less-secure passwords.

2. We reuse passwords across multiple sites.

   Again, memory plays a role here: An active web user may have *hundreds* of passwords to remember across every e-commerce site, social media platform, discussion forum, and news site he or she frequents. While security experts advise that we have different passwords on each site, it is

just not possible for most of us to easily remember so many different passwords—especially if we strictly follow the guidelines for hard-to-crack codes.

3. We share passwords.

   Almost half of us say we have shared passwords with friends, family, or co-workers. This is a conscious choice we make, usually because we assume we can trust the people we share the passwords with. This assumption, along with the convenience and ease of use that sharing brings, are important to us, and since we trust the people we share with, we tend to reason that our choices are unlikely to significantly compromise security, though it certainly could, especially if our passwords end up being used on a less-secure device or are stored on someone else's easily-accessible files. Further ...

4. We write down our passwords.

   This is fundamentally another memory issue. Many systems require people to choose passwords that conform to a particular set of guidelines. If it is too difficult for us to memorize such idiosyncratic passwords–which is often the case–we will write them down to make sure we don't forget or don't have to go through the long process of resetting the password when we inevitably do.

5. Mnemonics.

   When we try to follow password guidelines, we do some creative thinking to make them easier for us to remember. Mnemonics are one way to do this, and a good way, and so such tricks become common in our password constructions. To create mnemonics, we often use common names or words, encoding the first letters into our passwords, or replacing letters with representative numbers or symbols (e.g., o=0, i=1, e=3, a=4, s=5 or &, B=8, etc.). These can create solid passwords—if we create passwords that are personal and distinct, not if we rely on common phrases, as surveys show many of us do even in building mnemonics.