BIZCOMMUNITY

What do phishers do with your password?

By Andrew. B. Goldberg

17 Aug 2018

Online store account passwords are a common target for phishing attacks. As there are a number of widely-used and trusted brands, it is a good target for wide-scale phishing attacks, since people are likely to have an e-commerce account and feel the need to act quickly if they receive an email stating that there is an issue with their account.

Source: pixabay.com

But why would an attacker want your password? What could they do with this?

Here are some of the obvious and not-so-obvious uses for a stolen password.

Uses for a stolen password

A large-scale phishing attack is a common way for an attacker to steal your credentials. If a phishing email looks convincing enough, and the recipient is in a hurry, there is a good chance that the phisher will get at least one set of credentials for their trouble. So what comes next?

There are five possible scenarios of what an attacker might do with the stolen credentials.

1. Resale

The simplest reason that a phisher may steal your password in a phishing attack is for resale. Even if that particular attacker didn't have a use for your password, there are others who are looking to buy credentials on the Dark Net.

A password can be worth as much as US$10, meaning that a successful phishing attack could easily net an attacker hundreds or thousands of dollars. Some phishers will collect credentials just to make a quick buck.

#MobileCommerce: Understanding payment trends to ensure customers get what they want

Brendon Williamson 12 Jul 2018

2. Personal shopping

Many e-commerce platforms, users will commonly buy and sell things. One way for an attacker to get quick value out of a set of credentials is buying things to drain the value of the payment methods associated with the account.

If an attacker doesn't want to ship something to their home address, they can purchase something that can be instantly downloaded (music, videos, etc.) or have something delivered to a self-service parcel delivery service for pickup.

Since the attacker can pay for the fastest delivery method using the payment card attached to the stolen account, it's unlikely that the credential owner will notice the issue before it is too late. Common high-value items, like a laptop, could probably arrive and be picked up within a few hours (thanks to same-day delivery in many cities), and then resold secondhand to let the attacker cash out from their attack.

3. Data collection

Take a look at your Wish List and Purchase History. Is it possible that someone could learn anything about you from your online buying habits? By accessing your account, an attacker can collect a great deal of highly specific personal data about an individual.

While theft of a set of credentials may be possible with a simple mass phishing email, the data gathered from examining an account enables a phisher to craft a more targeted spear phishing attack that might give them access to more valuable information, like banking or corporate credentials.

Preparing for Black Friday - 8 lessons learnt from 2017

Graham van der Merwe 17 Jul 2018

All of this doesn't even take into account the personal information available in a user's profile. At a minimum, there will be a full name, email address, physical address, and partial credit card number information. Users may also have family sharing enabled or have sent gifts to friends or relatives, exposing the user's relationships.

An attacker can use this information to craft a more effective spear phishing campaign by masquerading as someone known to be close to the target and referencing a gift known to be sent.

4. Fraudulent sales

Another application of any password is sending money directly to an account under the attacker's control. Some attackers will post an item for sale on a platform for a large sum of money and then purchase it using a different account under the attacker's control. For example, the phisher could post a smartphone or tablet for sale and list it for hundreds of dollars without anyone being suspicious.

Using another account, the phisher can then "buy" the device so that money in one account is transferred to another without anyone having a reason for suspicion. There is very limited or no visibility over items being shipped between two users of its platform, so no red flags are raised when an item is never shipped.

If both accounts are owned and funded by the attacker, all this accomplishes is money laundering. However, if the attacker purchases the item using a stolen account, the result is that the value is just transferred into the attacker's account.

If both accounts are stolen, the attacker can even pull this off anonymously by performing the attack and then pulling the money out of the business before anyone becomes suspicious and attempts to track down the stolen money.

5. Password reuse

59% of people use the same password across multiple accounts. If your one password is the same as your password on another account, an attacker who steals one password may be gaining access to many other accounts. When passwords are stolen or breached, attackers commonly try combinations of email address or usernames and passwords across a variety of common websites.

While it may not be the end of the world if an attacker gains access to your Instagram account, what if your password is the same as your bank password? Or your email password?

Mobile banking Trojan modifications reach all-time high

6 Aug 2018

Email is a commonly used method of two-factor authentication and password reset. An attacker with your email password has complete control over every account that uses that email address as a password reset option, potentially including banking, social media, etc.

If you use the same password on multiple accounts, you should change them immediately. Consider using a password manager to help generate and store secure passwords so that you don't have to.

Protect yourself

There are many different ways that an attacker could take advantage of a stolen password, and there are probably even more clever ways to do so. Ultimately, what all of these methods have in common are that they're bad for the person whose account information was stolen.

You can increase the protection of your account with two easy steps. First, most credentials are stolen via phishing attacks. If an attacker can send a convincing email and trick someone into entering their credentials into an attacker-controlled website, the attacker now owns the target's account. By selecting a modern anti-phishing solution, and carefully scrutinising emails and websites before providing sensitive information, you can protect yourself and your account against phishers.

Enable two-factor authentication

Second, enabling two-factor authentication on your account is an important step in protecting it against attackers. Even if a phisher steals your password, it's useless if you've enabled two-factor authentication on your account. Your account is directly connected to your bank account and is full of sensitive information, so it needs to be protected. The Two-Step Verification option is an extra layer of security that will protect your account with both your password and your mobile.

Your online store account is a treasure trove for an attacker and might be exposed by a thoughtless click on a phishing email. Take these simple steps to protect yourself against all of the things that an attacker could do with your account password.

ABOUT THE AUTHOR

Andrew. B. Goldberg is chief scientist at [[https://www.inky.com/ Inky Phish Fence]].