Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

December 19, 2019
CS-09-2019

Storing Credit Card Information Online

OVERVIEW

Online shopping is one of the most popular and widely used purchasing options. Online retailers provide users with convenience in multiple ways like allowing account holders to store delivery addresses and credit cards, as well as enable certain ones as default. Default purchasing options are common in online shopping but storing credit cards or other bank account information incurs potential cyber related risk. The Michigan Cyber Command Center (MC3) has seen an increase in fraudulent purchases where malicious actors are targeting online retail accounts with stored default credit cards.

ATTACK VECTOR

If a malicious actor can gain access or compromise a victim's account, they will be able to make purchases using the stored credit card or steal the credit card information to use elsewhere. There are multiple attack vectors a malicious actor can use to compromise a victim's account, but the most popular is phishing.

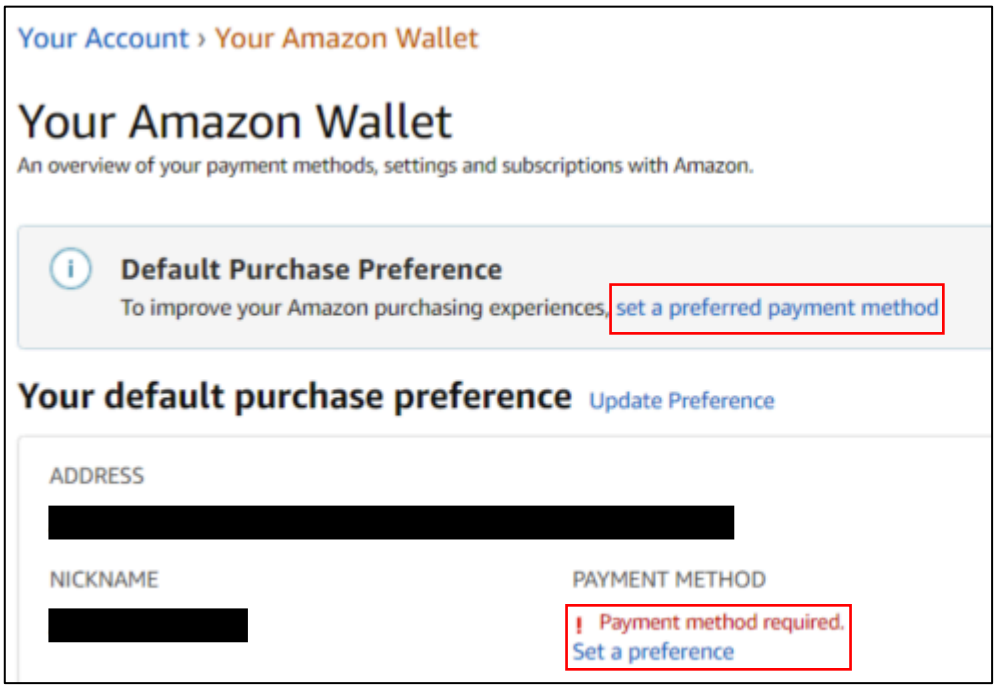

Image Source: Amazon.com

Malicious actors are hoping the stolen credentials from a compromised email address are the same for an online shopping account. If not, there is high a probability the compromised email address is also used as the recovery email address for a forgotten password which can be used to change the password and then gain access to the online retail account.

RECOMMENDATIONS

<u>Do Not Store Credit Cards Online:</u>

- Although it may seem like an inconvenience, the easiest way to prevent the risk of being exploited due to having stored credit card data is to not store credit card or bank account information online. If a malicious actor were able to compromise an online retailer account without stored banking information, it would be almost impossible to make fraudulent purchases.

Enable Multifactor Authentication (MFA):

- When storing banking information online, enabling some form of MFA is recommended. An example of MFA could be the requirement of biometric data such as a fingerprint before confirming a purchase or receiving a verification code to a previously verified phone number or application.

Set Up Alerts:

- When an item is ordered online, alerts with both the website and bank should be set-up to notify the user of the transaction. If fraudulent purchases are occurring, the earliest detection can prevent further financial loss.

REDUCING RISK OF COMPROMISE

Identify Phishing Emails:

- There are several different clues to look for when identifying phishing emails. For example, legitimate companies will never ask for the following information through email: bank account information, credit card numbers, PIN numbers, credit card security codes, mother's maiden name, personally identifying information, or account password. Do not directly respond to suspicious emails asking for these pieces of information.
- Review emails for grammatical or typographical errors which are more common in phishing emails.
- Check for spoofed senders. Emails can be spoofed to look as though they are originating from an online retailer like "@amazon.com". Additional steps such as checking the reply-to email address can identify a spoofed sender if the reply-to address does not match the received from address. It is best to go directly to the real website or call the website's Customer Services for help using a previously known phone number and not a number provided in a potentially malicious email.

Prevent Pivoting:

- In order to prevent a malicious actor from pivoting, or compromising secondary accounts, use complex unique passwords for every current online account, and never use the same password twice, no matter how old a password may be. If a malicious actor has gained access to one account, it will prevent them from easily gaining access to other accounts.
- Check for email forwarding rules. Once access is gained, malicious actors set up rules where all emails received to the compromised account are forwarded to another account the malicious actor controls. The MC3 has seen malicious actors creating forwarding rules and filters to delete emails from specific contacts after being forwarded. Forwarding or deletion rules could inhibit the ability to see when a recovery address is used to change the password of an online account.
- Ensure there are alerts set up for whenever a password is changed for an online account and use an alerting method separate from an email address.

Any additional questions or concerns can be sent to mc3@michigan.gov or 1-877-MI-CYBER.