Abuse/Misuse & PII

Daniel M Beck

UMGC – SDEV-360

July 7, 2020

Abuse/Misuse & PII

ATM Misuse/Abuse

How Customers can be Exposed to Misuse/Abuse

ATM Misuse/Abuse can start at the user of the ATM. The simplest form of stealing can be the attacker obtaining the PIN of the user and making cash withdrawals from their account using hidden cameras, or simply by standing nearby and watching as they enter their PIN. You might hand your information over to them without even realizing it, but consumers can take precautions. “Another technique is to alter the keypad with a device that records your PIN, possibly by placing a fake keypad over the original one. Heat-sensitive cameras on mobile devices can also help with figuring out your PIN” (Pritchard, 2019). At the ATM, it is important that the user ends their session or the session times out after a short period of inactivity so that no one will be able to come behind the user. The easiest way for users to mitigate these threats would be to pay attention to the ATM being used and use ones that they trust. Banks should keep a close eye on their ATM to make sure no altercations occur and that users can perform their transactions privately.

How Banks can be Exposed to Misuse/Abuse

A brute force, yet common way for attackers to gain access to the ATM, is by gaining access to the computer inside the ATM. This can be done by either gaining access to the cabinet housing the computer or remotely hacking into poorly encrypted wireless ATM networks. When hackers gain access to the internal computer, they can initiate many types of attacks.

They can access the security camera(s) of the ATM, erase the footage, and make it seem like they were never at the ATM. They can gain access to all the account of the users and see their balances, card numbers and routing information, among other details. They can install malware that allows them to continuously perform these attacks long after they have left the ATM. Since many banks set their ATMs up similarly, if one of their units get hacked, then there is a greater chance that their other ATMs have also been hacked.

Mitigating the Misuse/Abuse Threats

With banks losing millions of dollars every year to hackers, more should be done to help prevent the simplest of attacks. Hackers constantly evolve their tactics but Wagenseil states that banks could minimize these types of attacks "by insisting that ATM makers encrypt ATM hard drives, strongly encrypt communications with processing servers, upgrade machines to run Windows 10, disable common Windows keyboard commands, lock down BIOS configurations, use better administrative passwords and, last but not least, make the ATM computers harder to physically access" (Wagenseil, 2018).

Personally Identifiable Information (PII)

Rolling over fully vested money from one account to another

When working with a financial advisor to rollover my various 401k accounts into one account, I was asked by the account administrator of one of the accounts to provide the typical copy of a driver's license, security answers to my security questions and verbal confirmation of other PII. They also required me to send them my birth certificate so that they could make a copy to keep on file, with the promise that they would send it back. Unfortunately, the only option was to send them a certified copy of my birth certificate, in which has still not yet been returned. If I were to be working for this vendor, I would change the requirement of needing a birth certificate since this type of document can easily be mishandled or forgotten.

Paperwork needed for proof of relationship

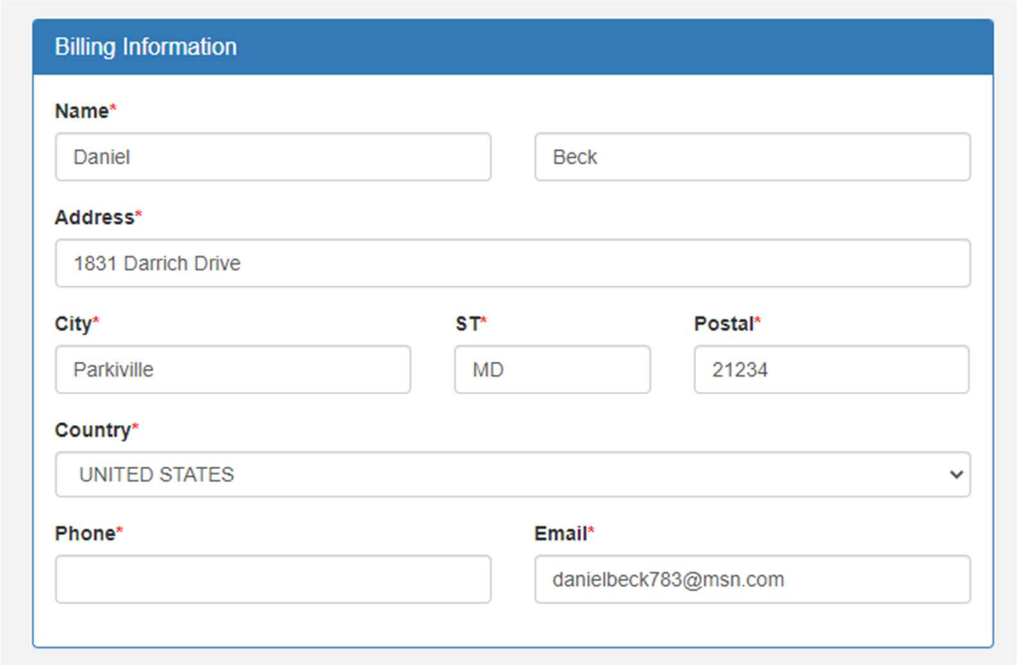
Recently, I have had to work on filling out an I-30 form need to prove my "relationship to an eligible relative who wishes to come to or remain in the United States permanently and get a Permanent Resident Card" (I-130, Petition for Alien Relative, 2020). While I understand the need to prove a relationship with someone, the list of items that the government wants to review is extensive. Some of these include:

- Two passport-style photos of petitioner
- Copy of petitioner's Driver's License
- Copy of petitioner's passport
- Copy of petitioner's birth certificate
- Copy of bank statement joint account
- Copy of joint insurance account
- Copy of joint cell phone bill
- Pictures of couple throughout the relationship
- Receipts of events done together

Since the government is requesting this material, there is no way to mitigate anything to prevent something from happening with the PII, even if I was to be working with them.

Men's baseball league must enter phone numbers

While signing up for a baseball league that I have been playing for the past couple years, I noticed something new with their registration portal.



Billing Information

Name*

Daniel

Beck

Address*

1831 Darrich Drive

City*

Parkiville

ST*

MD

Postal*

21234

Country*

UNITED STATES

Phone*

Email*

danielbeck783@msn.com

Figure 1, Screenshot of information being asked for by baseball league

As seen in figure 1, they now require everyone to fill out their phone numbers to complete registration. I understand needing the individuals address and email as they send newsletters out pertaining to the season. I can think of no reason for them to have phone numbers of anyone on file, as all contact and scheduling is through email. If I worked for this vendor, I may still ask for the phone number but would not make it a requirement. There are many people who do not like to give out their personal phone numbers if it is not necessary.

Conclusion

Many ways for individuals to stay protected from hackers is to protect themselves by staying aware of the information that they are sharing, and measures should be taken such as verifying the validity of the source they are sharing the information with. Sources must take measures from being hacked by increasing the security of their site such as the common CAPTCHA see on many sites when logging in or registering.

References

I-130, Petition for Alien Relative. (2020, June 29). Retrieved July 07, 2020, from https://www.uscis.gov/i-130

Pritchard, J. (2019, July 27). Skimmer Scams: What to Watch for and How They Work. Retrieved July 07, 2020, from https://www.thebalance.com/skimming-scams-315807

Wagenseil, P. (2018, November 14). Hacking an ATM Is Shockingly Easy. Retrieved July 07, 2020, from https://www.tomsguide.com/us/atm-hack-attack,news-28531.html