Use of Captchas on University Payment Sites
Audit & Consulting Services Review and Recommendations
Response to request from May PCI Committee meeting

Date: June 20, 2019

Captchas are pictures of distorted letters and numbers a website user sees and must enter in a field to prove they are a person legitimately completing a form on the site.

No standard exists for the use of CAPTCHAs on payment sites.

The Payment Card Industry Security Council and Data Security Standard provides guidelines on securing payment transactions.
The closest references in PCI-DSS are:

PA-DSS Controls 5.2.7-10
PCI-DSS Controls 6.5.7-10

For example PCI-DSS Control 6.5.8 states:

> Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
>
> Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that includes:
> - Proper authentication of users
> - Sanitizing input
> - Not exposing internal object references to users
> - User interfaces that do not permit access to unauthorized functions.

It is best practice to protect websites with fillable form fields from malicious attacks by humans and bots. CAPTCHAs offer a relatively simple way to protect payment sites from bot attacks. However, this method places the burden of proof on legitimate users, and it is not perfect. Therefore, site managers must ensure the test is quick and simple for the legitimate user and difficult, inconvenient, or unbeneficial to the potential attacker.

Multiple Solutions

Captchas are not the only solution to deter bot attacks. Other options include:

1. Games: website creators can use games that require the user to pass a test.
2. Honeypots: these are created by hiding an additional field from view. Legitimate users will not see it and will leave it blank. Bots complete all fields on the form. This method is not perfect because users with screen readers will “see” the field.
3. Verified sign-in: Forms that require users to sign in with their Facebook or Twitter account. Not all people have or want to use these accounts.
4. Time stamps: By recording the time to complete the form, site owners can determine bots from humans. Bots can complete a form instantaneously. However, if it is a returning user who completed the form earlier, their web browser may have the information stored and complete the form immediately for them.

5. Checkboxes: By labeling a checkbox, "I am human", legitimate users will respond to the question. To address bots, another checkbox is hidden and labeled, "I am not human." The bot will check all boxes while the human checks only the correct one.
6. Combinations of Captchas and/or above alternatives.

Audit Recommendation

University departments operating web facing payment sites should ensure that the tools provided by the PCI vendors are used in a practical manner to deter bot attacks and validate legitimate users of the site.