TREXIN INSIGHT PAPER
March 9, 2023

BALANCING USER FRICTION AND SECURITY

What is user friction?

User friction is any action that impedes a user from accomplishing a desired action on a website or app. Just like physical friction helps your shoes keep traction on a slick hardwood floor, digital friction can slow users from achieving their goals online—for example, making purchases.

User friction can happen for many reasons from inefficient design to bugs within the application. But in this case, we are examining friction due to security protocols that can make common tasks time-consuming and irritating to complete from a user experience perspective.

Financial institutions are focused on protecting their organizations from potential online risks and threats they face domestically and abroad. To protect customers, these financial institutions will design their applications to keep customers and their data safe, which often comes at the expense of their customers' user experience. Increased friction results in user frustration and the tendency to give up more quickly. For an online business, for example, this might result in fewer purchases, lowering its revenue and profit. Frustrated users also tend to seek out methods to reduce this friction by relieving configurable security settings when confronted with difficult processes which leaves these customers and institutions vulnerable to fraudsters.

While an institution should not compromise its own user security protocols, they can reduce this user friction without increasing security risk.

BALANCING SECURITY

An Example:

Let’s say you live in a single-family home. The first security layer would be the fence around the perimeter of your property. This fence is generally the weakest layer of protection to your property but also offers little value for potential criminals as they are only exposed to items within your property but outside of your house.

For the average homeowner, the second layer of security is the exterior of your home. You rely on locking your front door with a solid deadbolt, locking your windows, and closing your garage door even when you are home to prevent an intruder from gaining access to your home. These layers offer more difficulty for a potential criminal to break through to protect the valuables contained within your home.

The third layer of security for your home is your “safe” where you keep your most valued items. The safe requires knowledge of a passcode to gain access to and will be the most difficult layer for a potential criminal to break through.

These same layers can be applied to the cybersecurity world in protecting your digital assets.

Adaptive Risk Based Authentication

Using Multifactor Authentication relies on a user to provide two or more pieces of evidence to authenticate providing a high degree of secure authentication but creates a longer process for your customers. Adaptive Risk Based Authentication is a method that only requires a user to take additional steps to verify their identity when an authentication request is considered high risk while keeping the frictionless authentication process in place under normal conditions. Configuration of authentication based on the severity of the risk factors like geolocation risk, behavioral risk, or event risk is possible through adaptive authentication and provides your customer a more frictionless user experience.

Take for example a customer who normally logs into your system from Chicago. If they were to make an authentication request to access an application from a location they've never accessed from before or possibly a foreign country, this would be considered a high-risk situation and you might want to block the account instead of sending the notification to the consumer. This same logic would apply to a customer logging in from different devices or odd times in the day indicating potentially high-risk behavior. Although it is possible that these authentication attempts are valid, they should require a higher standard of verification.

Adaptive Authentication is evolving as Machine Learning can add more risk factors by studying consumer behavior over a period with historical data to enhance assessment. Hence, it provides a continuously updated layer of security against fraudulent attempts.

Step-Up Authentication:

Step-up authentication refers to the practice of requiring multiple levels of authentication to ensure that high risk actions involving sensitive information and transactions are not accessed by unauthorized people.

Let's apply this to a real application, such as a web-based banking application. Any user has access to navigate the public facing application as no real sensitive information is available at this point. If that same user wishes to access their account information, they will have to sign in with their credentials provided when they registered an account.

When the user logs in with the registered account, they get through the first layer of security and will have access to sensitive information. The user will also be able to perform certain tasks considered low risk such as checking their balance or looking through previous transactions. High risk actions such as Internal/External Transfers or Beneficiary Changes require stronger authentication than low risk actions. This is where Step-up authentication will activate a more secure authentication method to verify the user's identity to help keep user data safe.

HOW CAN TREXIN HELP?

It can feel like you are stuck between a rock and a hard place when it comes to balancing cybersecurity and the customer experience. Remember that the goal isn't to remove all friction, but to implement targeted and practical security measures that kick in at the right moment. Figuring out where that balance is can be challenging and often requires analysis and consultation with security professionals. That's where Trexin is here to help.

Click here to learn about Trexin's Cybersecurity Practice Area and how we can help you.

This TIP was written by Rick Herbas. Rick welcomes comments and discussion on this topic and can be reached at rick.herbas@trexin.com.