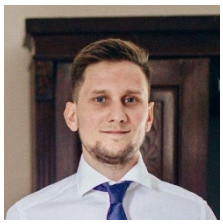
# Necessary Friction: The Theatrics of UX Security


*Contrary to conventional wisdom, there are times when making products harder to use can be beneficial. Here's how to use positive friction to enhance UX security and user trust.*



**By Nenad Ivanovic**
Nenad is a digital product designer and security expert who specializes in identity verification, e-commerce marketplaces, and fintech platforms. He has led design teams at creative agencies, IT firms, and startups, and has presented at conferences and events, such as UX Belgrade.

UX designers generally strive to make products easier to use, but there are circumstances in which adding friction improves product security. For instance, two-factor authentication makes login slower but can reduce identity theft. There are also occasions when implementing friction simply makes users *feel* safe: Animated progress bars don't protect personal data but may meet a user's expectations about the higher degree of processing power required in a secure environment.

As a product design manager for Freja, a digital security company under contract with the Swedish government, I routinely look for ways to harmonize usability with user safety. Sometimes that means incorporating features that users perceive to be secure. For example, most digital products can instantaneously compute complex data, but research shows that artificial loading times give users a sense that an advanced system is hard at work on their behalf. On the other hand, if designers are overly reliant on features that only appear to bolster security (known as security theater), they may lead users to believe that their information is safer than it is.

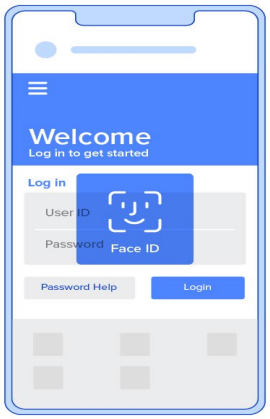
## Features That Enhance UX Security

Identity verification is a crucial aspect of UX security. Unfortunately, usernames and passwords aren't reliable authentication measures: In 2021, 85% of phishing attacks targeted user credentials. To combat this, designers are implementing security features that increase the time it takes for users to create and log into an account. For instance, multifactor authentication (MFA) requires multiple forms of identification at account creation or login. Most products that employ MFA require users to provide two of three credentials:

- A form of ID, such as a passport or driver's license, or a payment method, such as a credit card
- Unique information, like a password or PIN
- Biometric data, like a face, fingerprint, or retina scan

One way to streamline MFA while keeping users safe is to require a document selfie in which a user takes a photo or video while holding an official ID next to their face. Once the selfie is uploaded, companies either have an employee examine the user's face and ID for a match or use computer algorithms to determine authenticity.

Facial recognition is quickly becoming a popular security feature at login and beyond. For example, some banking apps use facial recognition to verify a user's identity when they want to access account details, sign e-documents, or transfer funds. And although many people use facial recognition alone to unlock their smartphones quickly, I recommend implementing the technology as part of an MFA strategy for heightened security.




Security measures that use biometric data, such as facial recognition, better safeguard users' identities, information, and funds against theft.

An easy way to verify a user's identity is by automatically logging them out at predetermined intervals ranging anywhere from half an hour to a few days. While some might find this method annoying, it can protect users who leave a laptop unattended, lose a smartphone, or forget to log out of a public computer.

There also will be times when users need to verify that they are the rightful owner of digital documents, such as event tickets and prescriptions. I helped Freja design a product that securely linked a user's digital identity (verified in our app) to their COVID-19 vaccine passport. This made the passport much harder to fake than the paper version or the preexisting digital version available in many countries. In Sweden and Denmark, for example, digital vaccine passports are not connected to other forms of identification and are typically accessed via a QR code.

Despite advancements in digital verification, some companies, including certain banks, still require users to visit a physical place to prove their identities, especially when applying for a loan. In such cases, staff members carefully review the user's appearance and ensure that it matches the photos on their identification documents. Some consider this security theater and argue that an employee could complete this task without the user present. But in-person visits can be a security enhancement because they safeguard against photo and video falsifications known as deepfakes, which are becoming harder to distinguish from authentic images. Additionally, an AARP Research survey found that 83% of adults age 50 and older aren't confident that their online activity and information are private. Providing these users with the option to have their documents reviewed in person can establish enduring product trust and loyalty.

Many digital products also store users' addresses, contact information, payment methods, and even medical histories. Given the stakes, you may think that implementing more security measures will lead to a more secure product, but that could easily create a frustrating user experience. Context is crucial. For example, if you were designing a crypto-trading app, you

might allow users to view token prices and trends without logging in since that information is easy to find on Google. But when users decide to purchase or sell tokens, you'd require them to log in using MFA. Different actions necessitate different levels of security.

## Security Theater That Makes Users Feel Safe

In some cases, designers rely on security theater to add friction and give users greater peace of mind. This practice can be beneficial—sometimes even necessary—as long as it isn't a substitute for UX features that genuinely protect users.

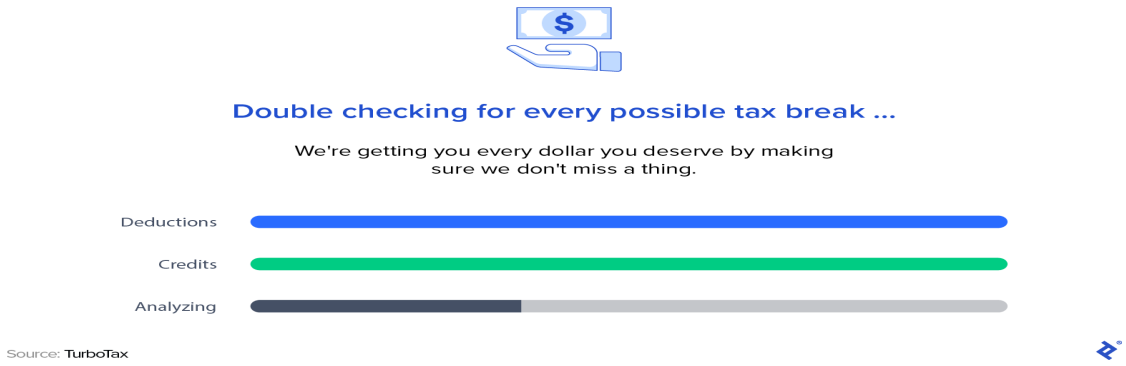
Some companies add unnecessary time to procedures to make them feel secure. TurboTax slows the processing of personal and financial information when a user is filing their taxes. Animated progress bars in conjunction with on-screen text assure users that the program is looking over every detail to ensure all possible tax breaks are applied. But TurboTax has already been verifying that data at every step.

Researchers who studied the TurboTax website's source code found that the progress indicators are preset. Once the animations start playing, they stop communicating with the site's servers. In addition, the progress indicators are the same for all users and always last for the same amount of time. The delay, graphics, and messages are theatrical methods meant to increase users' confidence that they're getting the biggest tax return possible—which is acceptable since TurboTax also employs data encryption and multifactor authentication.

Other companies add similar delays into a range of interactions. Wells Fargo slowed the retinal scanners on its app because users weren't sure they were working when they ran at full speed. Facebook's account security checks actually take milliseconds to process, but they force users to wait up to 10 seconds. Lender-backed mortgage apps, including one designed by Google Ventures, slowed their loan approval processes and added fake progress bars for credit checks because users didn't trust the instantaneous approval.

With the Freja eID app, we require users to hold their phones to their chip-enabled passports for three seconds to upload the information via near-field communication (NFC). In fact, the upload takes less than a second, but asking users to keep their phones steady for longer makes them feel the process is secure. We introduced friction into the document selfie as well: A static picture was all we needed, but users weren't convinced that was safe, so we added the step of having them turn their heads left and right.

All these companies, including Freja, have found that security theater—backed by actual security—has increased users' trust. As you work on UX security projects for your clients, remember that many users' mental models have not yet caught up to the fast pace of modern technology. Slowing things down can help users feel confident that a product is secure.




An illustrated rendering of TurboTax's fake progress bar and status message, which is identical for all users and always appears for the same length of time. The time delay, graphic, and text are examples of security theater, which can increase users' trust in the safety of a product.

# UX and Friction: A Symbiotic Relationship

UX security is a spectrum, and users have specific expectations of what security should look like: Sending a social media message should be fast and simple. Transferring $10,000 to someone else's bank account should not.

In interaction design, flow is often prioritized with the intent of helping users complete their goals as quickly as possible—but don't discount the importance of thoughtful friction that increases trust and safeguards users' valuable information.

### Further Reading on the Toptal Blog:

- Safe by Design: An Overview of UX Security
- How to Design for Maximum Product Trust
- Card Sorting: Better Information Architecture by Aligning with Users' Mental Models

*Link to article on Toptal design blog: https://www.toptal.com/designers/ux/ux-security-using-friction-to-design-safer-products*