JPTM PUBLICATIONS

Emerging Trends in Science & Technology Vol-I
eISBN : 978-81-999970-1-1 | ISBN : 978-81-999970-0-4
https://doi.org/10.67389/jptm.0626.etstv1.oa9

Enhancing Cybersecurity Through UI/UX Design

Anisha Das
Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida, Gautam Buddha Nagar, Uttar Pradesh 201304, India
anisha.mumbs@gmail.com

ARTICLE INFO

Article history:
Received 15 May 2026
Received in revised form 22 June 2026
Accepted 25 June 2026
Available online 12 July 2026

Keywords:
Usable security
Dark patterns
Financial technology
User interface design
Cybersecurity
Secure UX Framework

ABSTRACT

Nobody thinks about the designer when their bank account gets hacked. The blame goes to the hacker, the server, the compromised infrastructure, and something invisible. The point of failure is often sitting right there on the screen, in the font choice, the button placement, and the way a warning message was shown by someone who had a deadline and no security brief. Financial fraud is climbing not because encryption is weak but because the interface was never designed with protection in mind. This is the problem that cybersecurity research has largely failed to address, so this chapter is built around enhancing cybersecurity through UI/UX design. To understand this properly, the chapter looks at the problem from three angles. First, it looks at what academic research says - specifically a field called "usable security", which has been studying for years why good design and good security are actually the same thing, even though the tech industry has always treated them as separate jobs. Second, it looks at something called "dark patterns", a term for interfaces that are built to trick people. In financial apps, these tricks might look like a countdown timer that does not actually mean anything, fees hidden in small text, or a cancel button that takes six steps to find. These are not accidents; someone designed them that way on purpose. Third, the chapter presents real experience from creating a mutual fund app, where every design choice, including the colours chosen, the information arranged on the screen, and the text on each button, had a direct impact on whether or not actual users could trust the app with their money. What this chapter ultimately arrives at is not a list of warnings but a shift in perspective. For too long, the designer sitting in front of a Figma file has been handed a brief that says nothing about protection, nothing about vulnerability, and nothing about what happens to the person on the other side of that screen when the design gets it wrong. That has to change, and this chapter argues that it can, practically and immediately. The UI/UX designer in financial technology carries a responsibility that their job title has never formally acknowledged: they are, in every meaningful sense, a security practitioner. The wireframe is not just a layout; it is a decision about who gets protected and who gets exposed. To close that gap between what designers are asked to do and what they actually need to do, this chapter proposes the Secure UX Framework: a set of design principles that treat security not as a final checkbox but as the first question asked at every stage of the process. Starting from the very first sketch, protection is not something added to a finished product but something the product is built from.

1. Introduction

Anyone who has participated in sufficient design review meetings will recognise a familiar pattern. A prototype appears on screen. The team assembles. Comments follow: the hero image appears excessively corporate, the blue deviates slightly from brand guidelines, and the card spacing requires adjustment. Someone raises the question of whether the call-to-action button should display "Get Started" or "Start Now". Twenty minutes elapse. The meeting concludes. Throughout this discussion, at no point does anyone inquire whether the interface the team has spent considerable time evaluating is actually safe for the person who will ultimately use it.

This silence is not exceptional. It is, rather, the norm. Historically, cybersecurity and design have operated as distinct and largely disconnected disciplines. Cybersecurity has constituted the domain of engineers, infrastructure specialists, and those who develop encryption protocols in programming languages seldom encountered by design practitioners. Design, conversely, has concerned itself with colour psychology, user flows, and the experiential qualities of digital interfaces. These two disciplines have evolved in parallel for so long that the peculiarity of

their separation has become invisible to most practitioners on both sides.

The effects of this divide are observable in the available data. Despite substantial investment in technical security infrastructure, global financial fraud has not demonstrated a corresponding decline. Phishing attacks persist not because firewalls have weakened but because the interfaces users encounter daily - the screens to which they entrust sensitive financial information - were developed without adequate consideration of how they might be weaponised against the user. Encryption, however robust, cannot protect an individual who has been visually and interactionally guided into surrendering their credentials[1].

The present chapter addresses a question that cybersecurity scholarship has largely overlooked. It is not concerned with firewalls, encryption protocols, or password policies. Instead, it focuses on the screen, the layout, the colour scheme, and the microcopy. It examines the button positioned a few pixels too close to its neighbour, and the warning dialogue that users ignore because it appears identical to the numerous other warnings they dismissed the previous week. These are, and have always been, security decisions[2]. Yet they are made by UI and UX designers, frequently without those designers being aware that they are making security decisions at all.

This chapter seeks to bring that awareness into focus.

2. What Usable Security Actually Means

An academic field has been quietly advancing this argument since the mid-1990s. It is termed "usable security", and for those working in design or technology who have not encountered it, this fact alone communicates something significant about how seriously the industry has regarded it. Usable security, sometimes designated HCISec (Human-Computer Interaction Security), proceeds from a single uncomfortable observation: most security systems are designed by individuals who understand security thoroughly and understand human behaviour inadequately[3][4]. The result is systems that are technically robust and practically ignored. Complex password requirements cause users to write their passwords on adhesive notes affixed to their monitors. Two-factor authentication flows prove so cumbersome that users disable them at the earliest opportunity. Security warnings appear so frequently and in such identically formatted presentations that the brain ceases to process them as warnings and instead treats them as obstacles positioned between the user and the task they were attempting to complete. This is not a user problem. It is a design problem.

The central tension that usable security research consistently returns to is what researchers term the "security-usability trade-off". The principle is straightforward: the more barriers placed between a user and access, the more secure the system theoretically becomes, yet the more difficult it becomes to use. The uncomfortable element is this: when security is difficult to use, individuals find methods to circumvent it. They reuse passwords, remain logged in on shared devices, and dismiss warnings without reading them. They select convenience over protection on every occasion, not because they do not care about their security, but because the alternative of genuinely following every security protocol as designed would render it nearly impossible to accomplish anything[5][6].

A 2022 systematic review encompassing 55 empirical studies determined that this problem is not improving. Research in the field tends to concentrate on comparing security systems against one another rather than developing design guidelines grounded in how users actually behave. The gap between what security systems require and what human beings naturally do has been documented extensively. It has been addressed infrequently. While considerable research attention has been directed toward technical security domains—including lightweight cryptographic protocols for mobile and IoT devices [7], networking technologies and security threat countermeasures in IoT environments [11], secure random bit sequence generation for constrained environments [8], efficient encryption techniques for data transmission through IoT devices [12], privacy-preserving architectures such as federated learning [9], and secure signal processing in biomedical applications [10]; the interface layer through which end users actually encounter and

interact with these security mechanisms has received comparatively little systematic investigation. The encryption protocol may be robust, yet the screen that prompts a user to approve or deny a transaction remains designed without equivalent rigour.

What Usable Security proposes – and what this chapter argues specifically within the context of financial technology - is that this gap is not inevitable. It is a design failure. And designers can remedy design failures.

The practical implication for anyone constructing a financial interface is significant. Each time a user abandons a security step because it proved too complicated, that constitutes a design decision that created a vulnerability. Each time a warning goes unread because it was formatted identically to a promotional notification, that constitutes a design decision that created an opening. Each time an interface renders the risky path easier to follow than the safe one, that is not a neutral outcome. That is a choice. Someone made it - typically without realising what was actually being chosen [13][14].

Understanding this alters how a designer approaches their work. It is insufficient to ask whether something is easy to use; the question must include whether it is easy to use safely - whether the user can make the correct decision without requiring full comprehension of why it is the correct decision and whether the interface, through its structure and visual logic, is working for the person using it or quietly working around them.

That is the standard Usable Security research has been advancing toward for thirty years. It is also, not coincidentally, the standard that the most effective financial interface design has always sought to meet, even when it was not identified by that name [15][16].

Furthermore, machine learning models are increasingly being utilized to predict and manage security threats across various domains, providing proactive defense mechanisms.

For example, ensemble machine learning methods such as the Bagging Regressor with XGBoost have been shown to provide robust predictive capabilities in complex domains like the Indian power-energy market [20]. Ultimately, ensuring robust security in these market environments is as vital as the predictive models themselves, requiring a holistic approach that protects both data and the end users.

3. How Financial Apps Became the Most Dangerous Interfaces in the World

Opening any financial application and attending to the body's response reveals a particular quality of attention that activates the moment numbers representing personal finances appear on screen. Focus sharpens. Anxiety, if present, either rises or falls depending on what is visible in the initial two seconds. The screen is not being read in the same manner as a social media feed or a news article. The user is scanning for specific information - a balance, a transaction, or a confirmation - and the emotional state is directly connected to whether this information is located quickly and whether it appears as anticipated[17][18].

This psychological state - anxious, focused, and financially vulnerable - constitutes the environment for which every FinTech designer is actually designing. Not the relaxed, curious user exploring an application for the first time, but the individual checking whether their salary has arrived, the person attempting to complete a payment before a deadline, or the individual who received an alert they do not understand and is now navigating screens attempting to determine whether something has gone wrong.

This emotional context matters considerably for security. Research in behavioural psychology has consistently demonstrated that cognitive load - the mental effort required to process information - increases substantially under emotional stress. When an individual is anxious, their capacity to read carefully, evaluate options, and make deliberate decisions decreases significantly. They default to familiar patterns. They follow visual cues without questioning them. They trust what appears official because scrutinising it demands mental energy they do not currently possess.

This is why financial interfaces are uniquely dangerous. Not because they involve money, although that elevates the stakes considerably, but because the user arriving at them is almost invariably in a

heightened emotional state that renders them significantly more susceptible to being misled by a poorly designed interface and by a deliberately deceptive one in precisely equal measure.

This is why financial interfaces are uniquely dangerous. Not because they involve money, although that elevates the stakes considerably, but because the user arriving at them is almost invariably in a heightened emotional state that renders them significantly more susceptible to being misled - by a poorly designed interface and by a deliberately deceptive one in precisely equal measure.

Trust in financial interfaces is established and undermined through visual signals that operate faster than conscious thought. Studies in visual cognition indicate that users form a first impression of a digital interface in as little as 50 milliseconds - before they have read a single word. That initial judgement (safe or unsafe, trustworthy or suspicious) is based entirely on visual design: colour palette, typography, layout density, image selection, and the presence or absence of familiar trust signals such as security badges or brand consistency.

This is not theoretical. It constitutes the mechanism behind nearly every successful phishing attack targeting financial users. Phishing sites directed at banking customers do not succeed because they are technically sophisticated. They succeed because they are visually convincing. The layout corresponds. The colours correspond. The logo is positioned correctly. The user's brain, already primed to respond emotionally to financial interfaces, processes the visual signals faster than it processes the suspicion. By the time rational cognition catches up, the credentials have already been entered.

The designer who comprehends this is not merely an individual who makes financial applications aesthetically pleasing. They constitute the first line of defence against the most prevalent form of financial cybercrime globally. The question is whether the industry is prepared to acknowledge this and whether design education is equipping practitioners for that responsibility.

4. Dark Patterns: When Design Becomes a Weapon

In 2010, a UX designer named Harry Brignull coined a term for something that practitioners in the industry had been producing for years without a designated name. He termed them dark patterns: user interface design choices constructed specifically to benefit the platform at the expense of the user. Not by accident. Not through carelessness. Through deliberate, considered design.

The term has since entered regulatory language. The FTC defines dark patterns as manipulative design tricks and psychological tactics identified across e-commerce, cookie consent mechanisms, subscription services, children's applications, and additional contexts. What originated as a UX community conversation about ethics has transformed into a legal conversation about consumer harm. In financial technology, the stakes of that conversation are higher than in nearly any other industry (Reference: Pixflow Blog).

Understanding dark patterns properly requires distinguishing them from poor design. Poor design results from a team that did not test their interface adequately. Dark patterns result from a team that tested their interface extensively and subsequently employed what they learned to make it more difficult for users to make informed decisions. This distinction is consequential because the response to each is entirely different. Poor design is corrected. Dark patterns are selected repeatedly because they function effectively.

A review encompassing 642 websites and mobile applications determined that nearly 76 percent employed at least one dark pattern, with 67 percent employing multiple patterns (Reference: Federal Trade Commission). Within the context of financial applications specifically, the most common and most damaging dark patterns fall into several distinct categories, each possessing its own design logic and psychological mechanism.

Fake Urgency. A countdown timer on an investment offer. A notification stating "only 3 spots remaining" in a savings plan. A banner warning that an account will be affected if action is not taken within 24 hours. These are design choices that manufacture pressure

where none genuinely exists. They exploit the well-documented psychological principle of scarcity - the human tendency to assign greater value to items that appear limited - to push users into financial decisions they have not been afforded time to consider thoroughly. The design of fake urgency is deliberate and specific. The timer is prominent. The colour is red or orange. The copy is composed in language that implies consequence. Every element is engineered to bypass the deliberate thinking that financial decisions require.

Drip Pricing and Hidden Fees. A common "sneaking" practice involves concealing or delaying important disclosure information related to costs to influence consumer decisions, including appending non-optional charges at the final stage. In financial interfaces, this manifests as a fund with a management fee disclosed in small grey text at the bottom of a confirmation screen that the user has already decided to proceed past. It appears as a loan application displaying the monthly payment prominently while the total repayment amount resides in a collapsed section three scrolls below. The visual hierarchy - the deliberate choice of what appears large and what appears small, what is prominent and what is concealed - is executing the deception. No false information is provided; the fee is technically disclosed, but the design ensures it will not be observed (Reference: Federal Trade Commission).

Roach Motel. The term describes an interface that is straightforward to enter and nearly impossible to exit. Registering for a financial service requires four taps; cancelling it necessitates navigating to settings, then account management, then subscription details, placing a telephone call during business hours, awaiting a confirmation email, and then confirming again. This asymmetry is not a product oversight; it is a retention strategy presented as an interface. In April 2023, the FTC proposed the "Click-to-Cancel Rule," requiring that consumers be able to cancel subscriptions as easily as they register-mandating clear disclosures, express informed consent, and one-click cancellation. The fact that this rule needed to be established communicates everything about how normalised the roach motel pattern had become (Reference: Jasmine Directory).

Confirmshaming. The opt-out button stating "No thanks, I don't want to grow my savings." The notification permission screen where "Allow" appears as a large blue button and "Not Now" as small grey text in the corner. These are not neutral design choices. They are emotional manipulation presented as interface design. They employ shame, loss aversion, and the visual weight of design elements to pressure users into choices that serve the platform rather than themselves.

Misdirection. In financial interfaces, this is perhaps the most dangerous pattern of all because it operates at the level of visual attention itself. A complex fee structure presented alongside an animated graphic that draws the eye away from the numbers. A terms and conditions checkbox positioned such that the natural reading flow of the page carries the user past it without stopping. A "Confirm" button placed precisely where the user's thumb rests after scrolling, so that the next natural movement triggers the action before the screen has been fully read. These are not accidents of layout. They are the product of user testing - of observing precisely where people look, where they tap, where they hesitate - and then employing that knowledge against them.

What renders dark patterns in FinTech a security issue, rather than merely an ethical one, is their relationship to fraud. A user who has been conditioned by manipulative interfaces to dismiss warnings without reading them, to trust anything that appears official, and to act rapidly when an interface creates urgency is a user who has been specifically prepared to fall victim to a phishing attack. The dark pattern and the phishing site operate on the same psychological mechanism. One is legal; one is criminal. The interface design principles underlying both are nearly identical.

5. What Designing a Real Financial App Demonstrated

It is appropriate to share this experience briefly.

The brief stated, approximately, what most FinTech briefs communicate. Construct a website for a mutual fund company. Ensure it appears professional. Ensure

it is easy to use. The client was TNS, a mutual fund advisory firm. The individuals they sought to reach were not experienced investors with established portfolios and financial advisors. They were ordinary Indian families-people contemplating their child's education, their daughter's wedding, a house they hoped to purchase eventually. People who possessed funds to invest but had never invested previously, and who were quietly apprehensive about making errors.

That is not the category of user for whom most FinTech interfaces are designed. Most financial interfaces are designed for individuals who already comprehend what they are viewing-who understand what a SIP is before arriving on the page, who do not require reassurance but merely information. The brief did not articulate any of this explicitly. However, it was the first observation made when considering who would actually sit before whatever was constructed.

The initial decision concerned the hero section. This was not, or did not feel at the time like, a visual decision. The choice was to place people there. Not charts. Not percentage returns. Not a blue gradient with a padlock icon. People. A family. A couple smiling outside a house they had recently purchased. Parents with a child. Ordinary, recognisable Indian faces expressing something that financial language rarely expresses directly: that investing is not about numbers, but about the life one is attempting to build.

That choice constituted a security decision. Not in the manner cybersecurity textbooks employ the term, but in the manner that genuinely matters to the person on the other side of the screen. It communicated to the user, before they had read a single word of copy, that this interface understood what they were genuinely present for. That sensation of being recognised rather than processed is the foundation of authentic digital trust. And authentic digital trust is what causes a user to proceed slowly, read carefully, and make a considered decision rather than a panicked one.

The site's structure followed the same logic. Each service possessed its own page: mutual funds, SIP, and insurance. A user arriving without prior knowledge could follow a path, learn what mutual funds are, and understand what a SIP does-observing how the two connected before being asked to take any action whatsoever. The "Start Investing" button only appeared after that education had occurred. It was not being concealed; it was being positioned at the moment when clicking it would represent an informed decision rather than an impulsive one.

A calculator section was included. A user could enter a goal - saving for a wedding the following year, a budget of ten lakh rupees - and the calculator would display the monthly investment required to achieve it. This was not a feature added for engagement metrics. It constituted the answer to the question every first-time investor genuinely holds but rarely articulates aloud: is this for someone like me? Can I actually accomplish this? The calculator rendered the abstract concrete. It provided the user with a number that belonged to their life, not to a generic example.

A FAQ section was constructed from the questions real people ask when they experience anxiety about money. A contact form and a support number were included, positioned visibly rather than concealed in a footer. Nothing on that site was designed to rush anyone - no countdown timers, no "limited spots remaining," no forms demanding personal details before providing information. The entire design was constructed on a single principle that did not have a name at the time, but would now be termed Secure UX: a user who fully understands what they are doing cannot be easily deceived by someone purporting to offer the same thing.

That is the insight derived from that project. A phishing site operates by copying the visual language of a legitimate interface. The more generic and interchangeable that legitimate interface is, the easier it becomes to counterfeit. A distinctive, honest, user-first design is not merely superior UX. It is more difficult to counterfeit. Clarity, in financial design, constitutes a form of protection.

6. What Ethical FinTech Design Actually Looks Like

Having examined what deficient financial design resembles and what it costs those who encounter it, it is necessary to specify what the alternative actually entails. Not in the abstract, not merely "be transparent"

and "respect the user," but in the specific, practical, daily decisions that distinguish an interface constructed to protect from one constructed to exploit.

The first element is information hierarchy. Every visual layout makes a claim about what matters. Whatever is largest, whatever appears first, and whatever receives the greatest visual weight-that is what the designer is directing the user to attend to. In a dark pattern, this mechanism foregrounds the attractive figure and backgrounds the significant caveat. In ethical FinTech design, this is reversed. The fee sits adjacent to the return, at the same size and in the same weight. The risk disclosure appears on the same screen as the call to action, not linked away to a document that no user will open. Visual hierarchy constitutes moral architecture. The designer determines what the user sees first, and that determination is never neutral.

The second element is language. Financial services possess a long and largely undisturbed tradition of communicating in language that protects the institution rather than informs the user. Terms and conditions composed by lawyers for other lawyers. Risk disclosures phrased to be technically accurate and practically incomprehensible. Microcopy that employs precision to obscure rather than clarify. Ethical FinTech design treats language as a design material with the same seriousness as colour or spacing. Every line of copy on a financial interface should be answerable to a single question: does a first-time user, reading this under mild anxiety, understand what this means and what it is requesting them to do? If the answer is negative, the copy is not yet complete.

The third element is what may be termed patience in the user journey. Most financial interfaces are constructed around conversion-the moment the user commits, invests, subscribes, or agrees. Every element in the design propels toward that moment as efficiently as possible. Ethical design incorporates space before that moment. Educational content that requires nothing in return. A calculator that permits the user to view their own figures before deciding. A service page that explains what a product is before explaining how to acquire it. This patience is not commercially disadvantageous. Users who understand what they are doing convert at higher rates and retain at higher rates because their decision was genuine rather than manufactured. More significantly, a user who arrives at the decision point having genuinely understood the product is a user who is substantially more difficult to defraud, because they recognise what the legitimate interface looks like and how it should behave.

The fourth element is visible support. An ethical FinTech interface assumes its users will have questions, will encounter confusion, and will occasionally require assistance from a human being. It does not conceal the contact number. It does not obscure the support link in the footer at a font size that demands effort to locate. A visible, accessible support pathway - a FAQ constructed from genuine user questions, a contact form that is easy to find and efficient to use, a telephone number that is actually answered - constitutes both a service feature and a trust signal. It communicates to the user: we anticipate that you will have questions; we want you to ask them. That expectation, conveyed through design, transforms the relationship between the interface and the person using it from transactional to protective.

None of this necessitates a larger budget or an expanded team. It necessitates a different question at the commencement of the design process. Not "How do we move the user toward conversion?" but "How do we ensure the user understands what they are deciding?" That shift in the opening question transforms every decision that follows.

7. The Secure UX Framework

Everything examined in this chapter - the psychology of trust, the mechanics of dark patterns, the lessons derived from a practical financial design project, and the principles of ethical FinTech UX - converges toward the same practical gap. Designers working in financial technology require a method to integrate security thinking into their daily work that does not demand a cybersecurity qualification or a separate risk assessment procedure. They require something they can consult on a Monday morning, when constructing an onboarding flow, and employ to evaluate their own decisions before those decisions are implemented.

What follows is the Secure UX Framework: seven principles for FinTech designers, articulated in the

language of design rather than the language of security engineering.

One: Transparency First. Every fee, risk, and consequence must be visible where the user's eye actually travels, not where it is legally sufficient to position it. If a charge appears in a lighter font below the fold while the benefit appears in bold above it, that constitutes a layout decision that has created a vulnerability. Rebalancing the visual weight of difficult information is not detrimental to business. It represents the minimum standard of honest design.

Two: Reduce Cognitive Load. A user under financial stress processes information differently than a calm user. Complex journeys should be divided into clearly labelled steps. Friction should be removed from the comprehension phase, and the commitment moment should be reserved for when the user has genuinely had sufficient time and information to make an authentic decision. An interface that hurries a confused user is an interface that has created the conditions for a mistake - or for a fraudulent scheme to succeed in its place.

Three: Audit for Dark Patterns. Prior to any release, a dark pattern assessment should be conducted using the established taxonomy. Is opting out as visible and straightforward as opting in? Are all charges disclosed before the decision point? Is any urgency in the interface genuine or manufactured? This audit is not a legal exercise. It is a design quality check, equivalent to an accessibility audit or a usability test.

Four: Design for the Anxious User. The majority of individuals using financial applications are not financially confident. They are concerned about something tangible. Interfaces should be tested with people who are not comfortable with financial terminology. Observe where they hesitate, where they read and re-read, where they abandon the process. These are not edge cases. These are the individuals for whom the interface is actually intended.

Five: Make Security Signals Visible. Lock icons, encryption notices, two-factor authentication prompts, and privacy controls belong within the interface - not as decorative footer elements, but as active, legible, plain-language communications at the moments when trust is being established. A user who can see and understand the security of a legitimate interface is better equipped to notice when something is incorrect.

Six: Ethical Symmetry. Whatever is straightforward to activate must be equally straightforward to deactivate. This applies to subscriptions, data sharing settings, notification permissions, and automatic renewals. The asymmetry between the sign-up flow and the cancellation flow constitutes one of the clearest indicators of whether an interface was designed for the user or against them.

Seven: Map the Phishing Journey. Before finalising any financial interface, an attempt should be made to imagine a fraudulent version of it. If the design is sufficiently generic that a malicious actor could reproduce it inexpensively and convincingly, that constitutes a design problem with a security consequence. Distinctive, consistent, well-documented interfaces are more difficult to counterfeit. The design should be made specific enough that it cannot readily be mistaken for something else.

These seven principles do not replace security engineering. Encryption, authentication, and infrastructure all remain essential. What this framework addresses is the layer that precedes all of these: the screen the user actually encounters and the designer who determines what that screen does.

8. Conclusion

A version of this chapter exists that concludes with a call to action. That version advises designers to undertake cybersecurity training, to collaborate more extensively with security teams, and to incorporate a risk assessment step into their design process. All of this constitutes reasonable guidance. None of it captures the essential point.

The essential point is simpler and more uncomfortable. The UI/UX designer working in financial technology is already making security decisions. They are making them every day, in every layout choice, every line of microcopy, and every determination about where to position a button or how to phrase a warning. The question is not whether they are making those decisions; the question is whether they recognise it.

This chapter has argued that the interface is not merely a layer situated above a secure system. In financial

technology, it is the primary environment in which security succeeds or fails. Technical infrastructure - firewalls, encryption, and authentication protocols - can be functioning flawlessly while a user is simultaneously being deceived by a screen that instructs them to perform an action they would never undertake if they understood what was being asked. The screen is where the attack occurs; the screen is where the protection must also occur.

The field of Usable Security has been advancing this argument, predominantly in academic journals, for thirty years. Dark pattern regulation is rendering it in legal language. Fraud statistics are rendering it in the most expensive language of all. What remains absent is the design community articulating it in the language it comprehends most effectively - through the actual work of constructing interfaces that merit the trust users place in them.

The Secure UX Framework proposed in this chapter represents a beginning, not a conclusion. Financial technology will continue to evolve. AI-generated interfaces, voice banking, biometric authentication, and embedded finance - each of these introduces a new surface upon which the same tension between usability and security must be resolved. What will not change is the fundamental responsibility that accompanies designing for financial contexts. The individual on the other side of that screen is trusting that whoever constructed it had their interests in view.

That trust is not a UX metric; it is not a conversion rate or an NPS score. It is the actual relationship between a designer and the people for whom they design. In financial technology, earning that trust honestly - through clarity, patience, and design that protects rather than exploits - constitutes the most significant contribution a designer can make.

REFERENCES

[1] Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. ACM Computing Surveys, 54(8), Article 173. https://doi.org/10.1145/3469886

[2] Cranor, L. F., & Garfinkel, S. (2005). Security and usability: Designing secure systems that people can use. O'Reilly Media.

[3] Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, 169–184.

[4] Zurko, M. E., & Simon, R. T. (1996). User-centered security. Proceedings of the 1996 Workshop on New Security Paradigms, 27–33.

[5] Brignull, H. (2010). Dark patterns: Deception vs. user experience. https://www.deceptive.design

[6] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), Article 81. https://doi.org/10.1145/3359183

[7] Tiwari, A., et al. (2021). A review on conventional and lightweight security techniques in mobile and IoT devices. ResearchGate. https://www.researchgate.net/publication/347982871

[8] D. N. Gupta and R. Kumar, "Generating Random Binary Bit Sequences for Secure Communications between Constraint Devices under the IOT Environment," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-6, doi: 10.1109/INCET49848.2020.9154009.

[9] Gupta, D.N., Kumar, R., Kumar, A. (2022). Federated Learning for IoT Devices. In: Yadav, S.P., Bhati, B.S., Mahato, D.P., Kumar, S. (eds) Federated Learning for IoT Applications. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-85559-8_2

[10] Gupta, D.N., Anand, R., Ahamad, S., Patil, T., Dhabliya, D., Gupta, A. (2023). Phonocardiographic Signal Analysis for the Detection of Cardiovascular Diseases. In: Bhateja, V., Carroll, F., Tavares, J.M.R.S., Sengar, S.S., Peer, P. (eds) Intelligent Data Engineering and Analytics. FICTA 2023. Smart Innovation, Systems and Technologies, vol 371. Springer, Singapore. https://doi.org/10.1007/978-981-99-6706-3_47

[11] Deena Nath Gupta, Rajendra Kumar, Networking in IoT: Technologies Usage, Security Threats, and Possible Countermeasures, International Journal of Sensors, Wireless Communications and Control; Volume 11, Issue 6, Year 2021. https://doi.org/10.2174/2210327910666210106090826

[12] Gupta, Deena Nath, Rajendra Kumar, and Ashwani Kumar. "Efficient Encryption Techniques for Data Transmission Through the Internet of Things Devices." In IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks, edited by Ram Shringar Rao, et al., 203-228. Hershey, PA: IGI Global Scientific Publishing, 2020. https://doi.org/10.4018/978-1-7998-2570-8.ch011

[13] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Paper 534. https://doi.org/10.1145/3173574.3174108

[14] Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. Journal of Legal Analysis, 13(1), 43–109.

[15] Federal Trade Commission. (2022). Bringing dark patterns to light. FTC Staff Report. https://www.ftc.gov/reports

[16] Federal Trade Commission. (2023). Trade regulation rule on negative option and automatic renewal.

[17] Lindgaard, G., Fernandes, G., Dudek, C., & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! Behaviour & Information Technology, 25(2), 115–126. https://doi.org/10.1080/01449290500330448

[18] Tuch, A. N., Presslaber, E. E., Stöcklin, M., Opwis, K., & Bargas-Avila, J. A. (2012). The role of visual complexity and prototypicality regarding first impression of websites: Working

towards understanding aesthetic judgments. International Journal of Human-Computer Studies, 70(11), 794–811.

[19] Tiwari, D., Agarwal, S., & Singh, S. (2023). Machine Learning Models for Prediction of Energy Prices in Indian Power-Energy Trading Market. Proceedings of the 15th International Conference on Science, Technology and Management (ICSTM-2023), 117-127. https://www.researchgate.net/profile/Durgesh-Tiwari-6/publication/373524463_Machine_Learning_Models_for_Prediction_of_Energy_Prices_in_Indian_Power-Energy_Trading_Market/links/64f07bb64a2a2214db2833ff/Machine-Learning-Models-for-Prediction-of-Energy-Prices-in-Indian-Power-Energy-Trading-Market.pdf

[20] Tiwari, D., Agarwal, S., & Singh, S. (2024). Bagging Regressor with XGBoost Regressor as Base Estimator for Predictions in Indian Power-Energy Market. International Journal of Advanced Computer Science and Applications, 15(3), 450-458.