Risk Awareness and the User Experience

Richard F. Forno
Department of Computer Science and Electrical Engineering
University of Maryland Baltimore County
Baltimore, MD USA
rforno@umbc.edu

ABSTRACT

Although technology vendors prefer customers use their products according to pre-planned use cases, incorporating misleading user interfaces and crafting questionable decision points for users can induce them to make low-information decisions that may adversely impact their cybersecurity or operational postures. This Insight and accompanying presentation briefly offer industry-informed analysis and guidance on the professional and operational elements necessary to help overcome such issues to help users make more informed decisions about their digital well-being.

CCS CONCEPTS

• Human Centric Computing → Interaction Design

KEYWORDS

Risk; risk communication; user interface; cybersecurity; privacy

ACM Reference format:
Richard Forno. 2019. Risk awareness and the user experience. In *SIGDOC '19: The 37th ACM International Conference on the Design of Communication Proceedings, October 04–06, 2019, Portland, OR, USA*, 3 pages. https://doi.org/10.1145/3328020.3353918

1 INTRODUCTION

In the late 1990s, Mark Minasi [1] correctly observed that an unspoken policy of "release it now, fix it later" was the accepted, though problematic contemporary standard for software quality when developing mass-market software. In other words, being first to market and generating significant positive publicity, perhaps even with known but not disclosed problems is better than joining the market with a near-perfect product later and being perceived as an also-ran who is "late to the game."

Software companies, like all companies, are controlled by marketing campaigns. This means they strive to ensure customers use their products and services in ways that maximize profits through intended product designs and use cases that can induce customers to act in a certain way even if they don't want to. Such practices can foster deeper user lock-in to a particular product ecosystem or cause assorted cybersecurity or operational problems, among other potential and perhaps unconsidered consequences to customers.

Habermas [2] writes of the importance of informed participation in any decision-making process, noting that such activities must be conducted "in a way that provides each person with equal chances to exercise the communicative freedom to take a position on criticizable validity claims." Technology companies typically fail in this regard. For example, vendors may refer to security problems discovered in their products as "an issue" that "affects a limited number of users"—but then constantly revise that number upward. From a marketing perspective, this tends to minimize a vendor's list of public security problems—albeit by not calling them "security" problems.

Absent understandable and/or actionable information and knowledge about risks in platforms and products, people are at a disadvantage when making value decisions [1] about their digital well-being. Specifically, customers and potential customers may have difficulty researching what provides the best value for their money, comparing competing products or vendors, or understanding how their digital environment or capabilities may change as a result of their actions.

Cybersecurity typically relates to actions designed to ensure the confidentiality, integrity, and availability of information and information resources for authorized users. Through that prism, this Insight briefly explores how a user's interactions with, and decisions when using, technology can impact their cybersecurity or operational postures. It also offers some industry-informed recommendations on ways of addressing this concern.

2 ENABLING CONFUSION AND MANUFACTURING CONSENT

Apple prides itself on having the vast majority of its IOS- and MacOS-based devices running current software within a very short time after an update is released. From a security perspective, that is a good thing. However, the company tends to engage in misleading user interactions to induce users to update. As shown in Figure 1, after a new update is released, IOS displays a typical lockscreen which most users likely will bypass with their passcode via "muscle memory" once shown—and before reading the notice saying their phone will be updated that evening when charging.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
SIGDOC '19, October 04–06, 2019, Portland, OR, USA
© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9999-9/18/06…$15.00
https://doi.org/10.1145/3328020.3353918

Figure 1: Apple IOS Update Screen (2018)

However, there may be reasons a user does not wish to update their device now or "later" due to personal preference or known software incompatibilities. Unfortunately, Apple does not provide an option to permanently decline the update, preferring to periodically nag users instead and induce them into accidentally updating with a screen that looks like their phone's normal lockscreen. This means they may not even notice the fine print about the middle-of-the-night update after entering their passcode. Further, the "Remind Me Later" option, which only postpones another update reminder, is out of a user's direct line of sight.

Similarly, Figure 2 shows that Apple requires users to enable 2FA (2-factor authentication) to use its HomePod speaker. Users setting up a new HomePod and clicking through screens without understanding what 2FA entails may find themselves unable to use their other Apple services or devices until they reconfigure those items to use 2FA as well. This may be disruptive to their respective personal or professional workflows. From a traditional cybersecurity perspective, this can threaten the expected *availability* of a user's information and information resources.

While 2FA can raise a user's security against certain types of cyberattacks, forcing users to enable this feature when installing a new product is another way of inducing—if not forcing—user compliance with Apple's desire for its customers to use 2FA.

Figure 2: HomePod IOS Setup Dialogue (2018)

While increased security configurations typically are a good thing in principle, Apple requires 2FA to be enabled by users to take advantage of basic new product features. For example, users of IOS 12 are not able to synchronize their iMessages across their devices without enabling 2FA on all their Apple products and services.

In Figure 3, we note that Facebook engages in cleverly-framed user dialogues to induce customer compliance with how the company prefers customers use its platform.

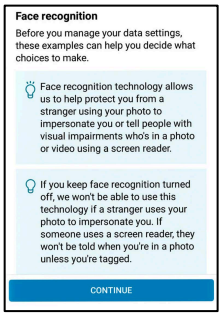

Figure 3: Facebook Face Recognition "Warning" (2018)

When Facebook introduced its facial recognition capabilities for pictures in 2018, users were presented with a prominent dialog box framing this new capability as a method of protecting the user's identity. In essence, Facebook used cybersecurity as the inducement for users to enable this feature. However, the announcement minimized the fact the company planned to scan every photo in the user's account for various undisclosed analytical purposes. From a traditional cybersecurity perspective, this practice can threaten the *confidentiality* of a user's information on the platform.

Deceptive user interfaces also may lead users into making decisions that place themselves at greater cybersecurity or privacy risk. In 2018, Facebook was sued for violating European GDPR regulations by presenting users with persistent message notifications allegedly designed to induce users to agree to their new GDPR ToS. Per the court complaint [3]:

> …the consent page included two fake red dots that indicated that the user has new messages and notifications, which he/she cannot access without consenting – even if the user did not have such notifications or messages in reality. The only option for a user was therefore to accept the new terms and privacy policy, or to delete the account. There was no option to disagree, opt-out or say no in any other way, shape or form.

These brief examples demonstrate some of the ways that users are influenced through interface design to induce them into complying with a vendor's desired use-case for its products. Oftentimes user decisions are made without knowing the possible cybersecurity or operational consequences until problems occur afterward. What benefits and conveniences a user might gain from such new products or features tends to outweigh thoughts of what they may lose or place at risk by their decisions.

3 RECOMMENDATIONS

The cybersecurity profession is only now beginning to acknowledge and/or incorporate non-technical disciplines and perspectives, such as human factors (e.g., Dark Patterns [4]) when determining and communicating operational risks to users. The examples shown earlier indicate that there is significant room for improvement in how cybersecurity and related operational risks are presented to users in order for them to make informed decisions. With that in mind, this Insight offers some recommendations framed within the cybersecurity and operational contexts and informed by firsthand industry experiences.

3.1 Fostering Trust through Informed Consent

Trust presents variations on the fundamental question of how to interact comfortably with others, including strangers; it touches some fundamental issues of human society and individual psychology, and is predicated by social perceptions. While fostering trust is crucial for any vendor to enhance its marketplace perception and customer satisfaction, the potential for losing that trust must not be ignored. As Slovic [5] rightly argues, trust is easier to destroy than to create, and while although trust relationships take a long time to establish, they may be destroyed very quickly. Unfortunately, once lost, trust never may be regained, or regained with the same degree it had formerly. Moreover, since distrust feeds on itself, it can color one's view of events and inhibit the development of future trust relationships.

Ideally, customers trust their products and product vendors. However, inducing customers into doing something that could disrupt their digital well-being is not conducive toward that goal. Despite marketplace pressures, products must be designed from the start to minimize user confusion and offer clear, understandable information leading to informed decisions. This requires professionals with a solid understanding of not only the underlying technology (such as software developers and engineers) but more so the human cognitive factors associated with how users interact with the product. Computing-related disciplines that can help this process include communicators, visualizers, and technical HCI or UX/UI professionals. But they must work alongside practitioners and scholars from the social sciences and humanities to address these issues in a holistic and meaningful way.

4 CONCLUSION

Companies are under commercial demands to expand their customer base and profits. Nevertheless, cybersecurity functions should not be conflated with the ability to use new and unrelated product features or as the unspoken basis for creating greater lock-in to a given product. Section 2 described some of these techniques and the ways that users are induced to make decisions that can potentially disrupt their digital activities.

More importantly, users themselves must take steps to become better informed about their technology usage and think critically about how a decision to embrace a new product or feature may lead to future cybersecurity or operational problems. In addition to basic technology literacy, skills like independent research and critical thinking must be taught from an early age to help establish a future user population comfortable enough to question things and research items of concern or interest. This will hopefully enable them to be better prepared to make informed decisions about their technology regardless of what is presented on their screens.

REFERENCES

[1] Mark Minasi. 1999. *The software conspiracy: Why companies put out faulty software, how they can hurt you and what you can do about it.* New York: McGraw-Hill.

[2] Jurgen Habermas. 1996. *Between facts and norms: Contributions to a discourse theory of law and democracy.* Cambridge, MA: MIT Press.

[3] Garett Sloane. 2018. Facebook and Google get their first GDPR complaint and its over 'forced consent.' *AdAge.Com.* https://adage.com/article/digital/facebook-google-gdpr-complaint-forced-consent/313660.

[4] Dark Patterns https://darkpatterns.org/.

[5] Paul Slovic. Perceived risk, trust, and democracy. *Risk Analysis* 13, 6 (1993), 675-682.