HBCS: Security and Usability Trade-offs

u5539006

November 2024

Contents

1 Introduction

This report follows the model proposed by Kainda et al. (2010) to analyse Microsoft's Outlook email management system. Using the method shown in Figure 1, both usability and security scenarios will be discussed from the perspective of a legitimate user. Outlook is a web and application-based system that allows users to send and receive emails, and manage their calendar. It is widely-used (6sense, 2024) in educational and business settings, and therefore needs to be both usable and secure.

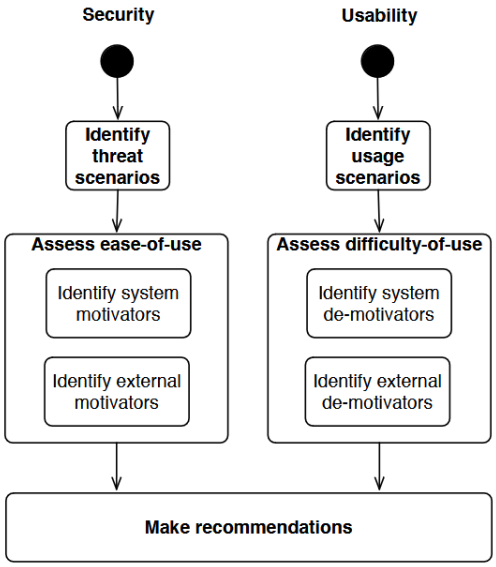

Figure 1: Process for security-usability analyses, proposed by Kainda et al. (2010)

2 Identifying and Assessing Usage Scenarios

2.1 Viewing Inbox and Reading Emails

A standard user would use the Outlook application to read their emails, using the initial interface. This would involve scrolling down the list of emails until they find the relevant one and selecting it, opening it in a larger panel to the right. However, there are several de-motivators affecting certain users because of the lack of inclusive design features application-wide (Figure 2). Accessibility options, even common ones such as high-contrast mode, or the ability to increase text size, are absent from this application, despite the WCAG 2.1 guidelines which emphasise the need for these options in digital interfaces (W3C, 2021). Since around 20% of the world's population use accessibility options online (Halpin, 2024), and Outlook had 400 million users as of 2022 (Silva-Payne, 2022), at least 80 million users will find it difficult to use, and thus frustrating, which flags both satisfaction and efficiency as prevalent de-motivators. There is, however, an 'Immersive Reader' which can read emails with an increased contrast and font size, but this is both hidden inside a menu, meaning users with less technical skill or poor eyesight may not find it, and is only available for email content.

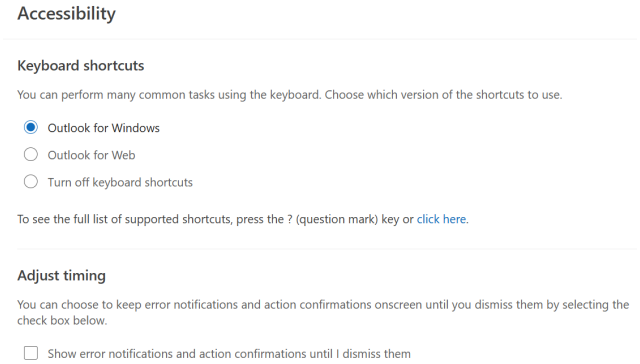

Figure 2: Lack of accessibility options in Outlook settings.

2.2 Sending an Email

Another legitimate use of Outlook is to send emails. This is enabled once the user selects the 'New mail' option in the 'Home' tab of the navigation bar, opening a new panel to the right where users can write and configure their email before sending it. Writing a simple email is easy, but there are still several de-motivators. The many buttons and icons in the toolbar that allow a user to format their email, or configure the sending options, can be overwhelming to users (Figure 6, appendix A). This leads to ineffectiveness, where the user simply ignores all of them, inefficiency, where the user attempts to understand all of them (which takes a long time, according to Hick's law (Liu et al., 2020)), or dissatisfaction, where the cognitive overload of understanding and deciding what to use causes decision fatigue (Schwartz, 2005), and does not follow Nielsen's heuristic on "aesthetic and minimalist design" (Nielsen and Molich, 1990) to prevent interface clutter. Another de-motivator is the inefficiency in another respect: email templates. Widely supported email templates such as .msg (Outlook's previous proprietary format) and .eml files (Smith, 2015) aren't supported by Outlook (new) for creating new emails, increasing the time and mental effort required.

2.3 Creating Calendar Events

Legitimate users may use Outlook to manage their calendar: adding events they may have been invited to via email, or by creating the events manually. To manually create an event, once on the Calendar page, the user must select the 'New event' button and fill in the required details e.g. title, date, time etc. However, more complex events may require more information and for users wishing to add an attachment, no drag-and-drop functionality is given. According to a study by Icons8, in a sample of 13 people, 8 used drag-and-drop

intuitively compared to 5 who chose to click and select (Icons8, 2020). Having drag-and-drop functionality not only increases the user's satisfaction because of the visual presentation but also allows the users to have greater efficiency - a direct implementation of ISO 9241-11 (for Satndardization, 2018), making task completion more efficient by aligning with user's mental models. Therefore, not having this feature de-motivates users about using this tool. Secondly, when a user wishes to view details about the event, they select it. This opens a small, minimised view of the event (Figure 3) and to view more details, more buttons must be clicked. This is another de-motivator for efficiency and satisfaction for users viewing detailed events.

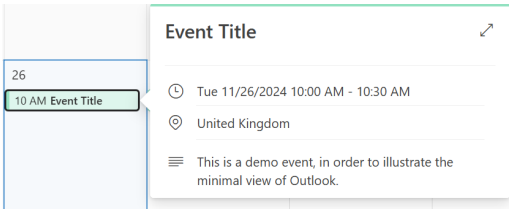

Figure 3: The minimal view available to users when they select an event.

3 Identifying and Assessing Threat Scenarios

3.1 Sending an Email to an Unintended Recipient

When sending an email through Outlook, there is a very handy usability feature that autocompletes recipient email addresses based on the partial email address the user has already typed in, saving them typing the rest. However, this can make it very easy to select the wrong recipient from the autocompleted list, whether they are of the same name or not (see Figure 4). According to a study conducted by Virtru, approximately 70% of sent emails from businesses include "sensitive information" (information labelled as sensitive by client administrators) (Leader, 2021). Another study, by VIPRE, concludes that 78.5% in employment "send an email to the wrong recipient at least once a year, and another 10.8% once a month" (Bloxberg, 2024). This is because of a lack of attention on behalf of the user, but also a lack of vigilance if, for example, confidential information was sent to an unintended recipient by BCC'ing or CC'ing, or by including it as contextual information.

3.2 Staying Logged-in on a Public Computer

40% of users of email management software use Outlook, according to 6sense (6sense, 2024). This means that users will inevitably use public computers, or non-personal computers, to access their Outlook accounts.

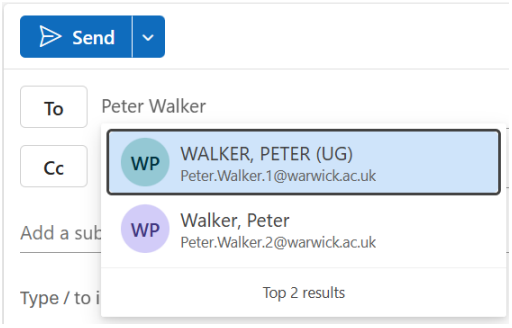

Figure 4: Two users with the same name, where either could be the intended recipient.

When signing into Outlook, if using the desktop application, there is no additional security once a user has signed in. Anyone reopening that application will still be logged into Outlook. When signing into Outlook online, an option is given to the user to stay signed in, and agreeing to do so is both the default and highlighted option, grabbing user's attention more easily. Users in a rush may click this option, or hit enter, before thinking about how this affects them. If so, Outlook will keep them logged in online for up to 90 days before requiring password re-entry. Closing the browser will not log them out either. If users are not maintaining constant vigilance and attention while signing in, they introduce session hijacking risks by inadvertently allowing another user to access their Outlook account.

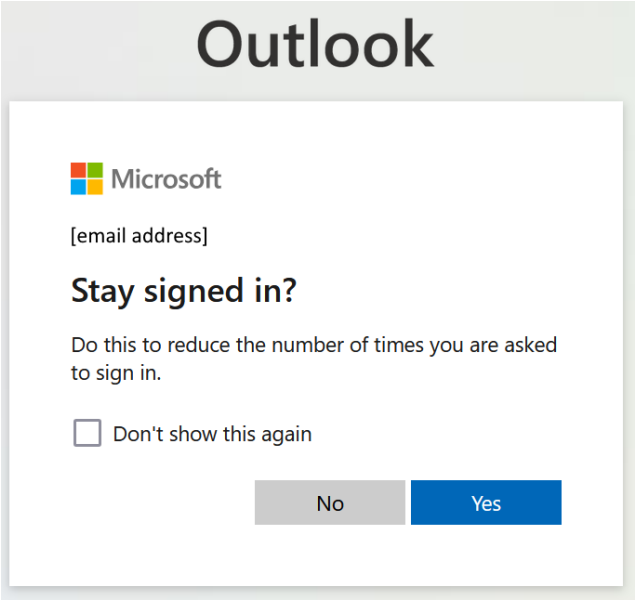

Figure 5: The highlighted option is to stay signed in when using Outlook online.

3.3 Clicking a Link on a Phishing Email

When a user receives an email that looks like it might be spam, Outlook will often display a small warning at the top of the email. Despite this, the spam filter isn't

100% accurate and may give false positives/negatives about emails, reducing user's trust in the tool. A study by Asangi Jayatilaka (2021) concluded that only 37% of users consistently check links in the body of emails before clicking them, which is the most common way to steal user information (Zainab Alkhalil, 2021). It was also concluded that, on average, 91% of users who clicked the links would give away their personal information. Since humans are naturally trusting (Peter A. Hancock, 2023), it is necessary for users to be constantly vigilant when inspecting and reading emails, even from trusted sources, which is unlikely, as this causes cognitive overload and users eventually reduce their vigilance.

4 Risk Matrix and Proposed Recommendations

Scenario	Impact	Probability	Severity	Recommendations
User finds the system difficult to read.	2 (It is still possible to use despite these issues, just requires increased cognitive load.)	2 (Doesn't affect 80% (Halpin, 2024) of users on average.)	4 (Low)	Allow users to select a high-contrast theme for Outlook, such as using yellow text on a black background, and allow them to increase the font size. It is recommended to implement this in a similar way to web browsers, according to Jakob's Law (Yablonski, 2024): a shortcut of Ctrl+ and Ctrl- and also having a menu on the application where users are able to change the zoom percentage. This will increase user satisfaction and efficiency, as they will find the application easier to use.
User has to repeatedly create emails rather than using a template.	2 (It is still possible to copy content into the body of the email, just less efficient.)	3 (Many users do not send emails using a template, instead using them for one-off communication.)	6 (Medium)	Allow users to import saved messages as .msg and .eml files and send the edited emails, improving efficiency when users are sending templated emails. This could be added as another option when creating a n email to allow users to 'Import Templates'.
User is overwhelmed by configuration options.	3 (Makes it difficult to find specific settings that a user may require.)	2 (Users may be familiar with a few common items, and only need to locate new ones.)	6 (Medium)	It is recommended that the formatting and configuration toolbar used when sending an email to be compiled into labelled drop-down lists for user convenience, thus making it less overwhelming, and conforming to Gestalt's principles of design proximity principle (Khatun, 2024).
User doesn't understand how to add attachments to an event.	2 (May mean that other attendees cannot access crucial resources.)	1 (Most users will find a way to attach files that isn't drag-and-drop.)	2 (Very low)	Allow users to drag-and-drop attachments into events, whether that's dragging the attachment into the event details or just onto the event listing in the calendar, to conform with ISO 9241-11 (for Satndardization, 2018), improving both user satisfaction and efficiency.
An email is sent to an unintended recipient.	5 (Email could contain highly sensitive/confidential information.)	2 (Users tend to double check recipients when important data is being sent.)	10 (High)	Increase the size of the email address in the autocomplete results, and make it bold, reducing the required attention to ascertain the correct email. It is also recommended to, instead of highlighting the name, highlight the email address and have the name as secondary information beneath it.
User stays logged-in on a public computer.	5 (Unauthorised user could access confidential data in initial user's emails.)	3 (Very easy to remain logged-in by accident, and many users use public devices.)	15 (Very high)	Make the default option, when logging-in, to not stay logged in, in a way that is psychologically acceptable to users. This should use an unchecked checkbox in the same window as password entry, so it isn't on a separate screen, therefore requiring no vigilance from users, since the default option is secure. Also, change the session timeout time to significantly less, such as a few days or 24 hours.
User trusts a phishing email and clicks on a malicious link	5 (Bad actors could steal personal or confidential information.)	3 (Humans are naturally trusting (Peter A. Hancock, 2023) and will want to help out/obey.)	15 (Very high)	Have a larger alert for detected phishing emails, reducing the attention necessary for the user to process the information, and flag emails from new senders. It also recommended to have an alert when clicking on links from emails directly, which includes the URL it is redirecting to in bold, in order to force user vigilance.

References

Ronald Kainda, Ivan Fléchais, and A.W. Roscoe. Security and usability: Analysis and evaluation. In *2010 International Conference on Availability, Reliability and Security*, pages 275–282, 2010. doi: 10.1109/ARES.2010.77.

6sense. Microsoft outlook - market share, competitor insights in email management, 2024. URL https://6sense.com/tech/email-management/microsoft-outlook-market-share.

W3C. *Web Content Accessibility Guidelines (WCAG) 2.1*, 9 2021. URL https://www.w3.org/TR/WCAG21/.

Michael Halpin. Assistive technology: Who needs it?, 2024. URL https://reciteme.com/news/assistive-technology-who-needs-it/.

Gino Silva-Payne. Gmail vs outlook: Which is the best in 2023?, 2022. URL https://www.emailmeter.com/blog/gmail-vs-outlook.

Wanyu Liu, Julien Gori, Olivier Rioul, Michel Beaudouin-Lafon, and Yves Guiard. How relevant is hick's law for hci? In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–11, 2020.

Barry Schwartz. *The paradox of choice: why more is less*. HarperCollins, 2005. ISBN 0060005696;9780060005696;.

Jakob Nielsen and Rolf Molich. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, page 249–256, New York, NY, USA, 1990. Association for Computing Machinery. ISBN 0201509326. doi: 10.1145/97243.97281. URL https://doi.org/10.1145/97243.97281.

Paul Smith. Standard file types, 2015. URL https://www.pscs.co.uk/manual/email-file-types.html.

Icons8. Drag-and-drop vs. click. are they rivals? [usability study], 2020. URL https://blog.icons8.com/articles/drag-and-drop-vs-click-are-they-rivals-usability-studies-revealed/.

International Organization for Satndardization. *ISO 9241-11:2018(en) Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*, 03 2018. URL https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en.

Megan Leader. How much sensitive data is your organization sharing?, 2021. URL https://www.virtru.com/blog/data-centric-security/risk-calculator.

David Bloxberg. Email sent to the wrong person? how to prevent data leaks, 2024. URL https://vipre.com/blog/email-sent-to-wrong-person/.

M. Ali Babar Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage. Falling for phishing: An empirical investigation into people's email response behaviors, 08 2021.

Liqaa Nawaf Imtiaz Khan Zainab Alkhalil, Chaminda Hewage. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 2021. doi: 10.3389/fcomp.2021.563060.

Alexandra D. Kaplan Kimberly Stowers John Christopher Brill Deborah R. Billings Kristin E. Schaefer James L. Szalma Peter A. Hancock, Theresa T. Kessler. How and why humans trust: A meta-analysis and elaborated model. *Frontiers in Psychology*, 14, 2023. doi: 10.3389/fpsyg.2023.1081086.

Jon Yablonski. *Laws of UX*. " O'Reilly Media, Inc.", 2024.

Tafura Khatun. Exploring the fundamentals of gestalt theory in visual perception. 02 2024.

A Outlook (new) Feature Overload (2.2)

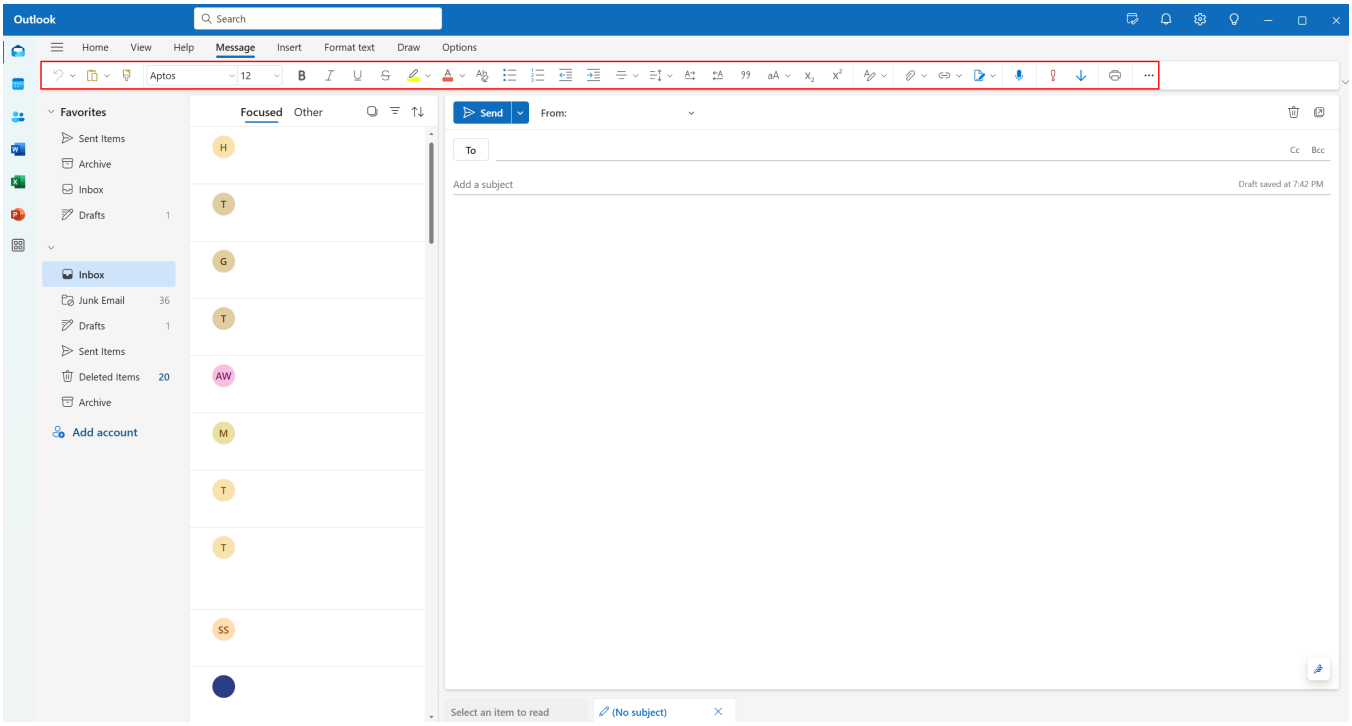

Figure 6: Overwhelming number of formatting and configuration options for a draft email.