

WEBSITE'S ANALYSIS BASED ON HEURISTIC PRINCIPLES

Word count 1630



JULY 15, 2025

W24059727

Abdulmajeed Almutairi

Task 1 – Website Inspection Using 3 Heuristic Principles

Help Users Recognize, Diagnose, and Recover from Errors (Principle 9)

Definition: According to Nielsen (1994), Principle 9 requires systems to deliver clear, constructive error messages that enable users to identify issues, understand their cause, and take corrective action. This heuristic is a recognized industry standard for enhancing user autonomy and system usability, as endorsed by ISO 9241-151:2008.

Evidence: The Barclays login page exemplifies this principle with a sophisticated error-handling system. When users leave required fields like last name or membership number blank, the interface highlights these fields in red and shows accurate messages: "You must enter your last name" and "You must enter a membership number." A clear error summary at the top, "You have 2 errors to correct before you can proceed," summarizes all problems for easy identification. Step-by-step screenshots demonstrate: (1) the blank login form at the beginning, (2) the error state with highlighted fields and messages, and (3) the "Don't know your membership number?" link to a comprehensive recovery guide—best practice in financial web design.

The screenshot displays the Barclays login interface with several annotations. At the top, a pink box labeled "errors summary" contains the message: "You have 2 errors to correct before you can proceed" followed by two bullet points: "You must enter your last name" and "You must enter a membership number". Below this, the login form is titled "How would you like to log in?". It includes a link for "Not registered for Online Banking? Register now." and three input fields: "Membership number", "Card number", and "Sort code and account number". The "Last name" field is highlighted in red, with a red box labeled "errors message" pointing to the error text "Error: You must enter your last name". The "Membership number (12 digits)" field is also highlighted in red, with a red box labeled "Recovery" pointing to the error text "Error: You must enter a membership number" and a link "Don't know your membership number?". The "anotely.com" watermark is visible in the bottom right corner.

Figure 1 Diagnosis and Recovery at Login Page

Evaluation: This deployment goes beyond simple error notification by providing actionable feedback and a recovery path, reflecting Nielsen's emphasis on user empowerment. The uniform, user-sensitive design minimizes cognitive load and instills trust, an essential ingredient for banking sites. This practice establishes a peer group standard by predicting user needs and providing successful recovery, showcasing deep usability innovation.

Help and Documentation (Principle 10)

Definition: Nielsen (1994) describes Principle 10 as the provision of readily accessible, context-sensitive assistance and documentation to facilitate user activity. This is a usability benchmarking principle, supported by W3C guidelines for accessibility (W3C, 2023), to ensure inclusivity and self-help.

Evidence: Barclays provides outstanding support via the "Help & FAQs" section in the footer, covering areas such as fraud reporting and cash access through clickable links. The login page has "Not registered for Online Banking? Register now" and "Don't know your membership number?" links as shown in Figure 1, with the second linking to a multi-step recovery process. Further assistance is provided through live chat and phone options under "Help & support" in the navigation menu.

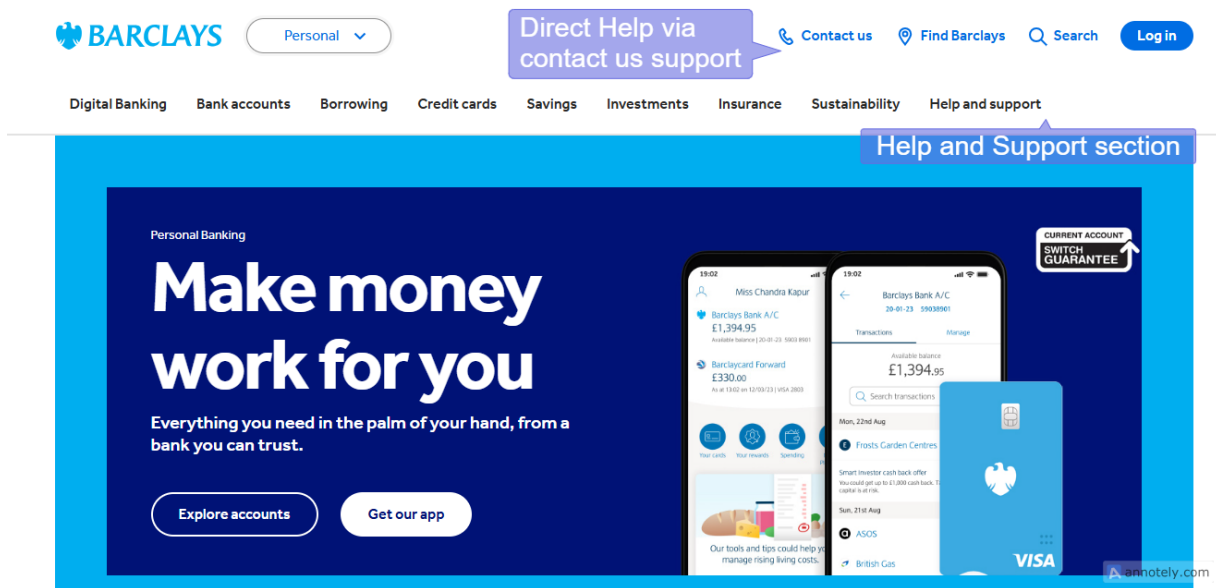


Figure 2 Navigation Menu Live help Options.

The screenshot below shows the footer help menu with support services and reporting illegal activities.

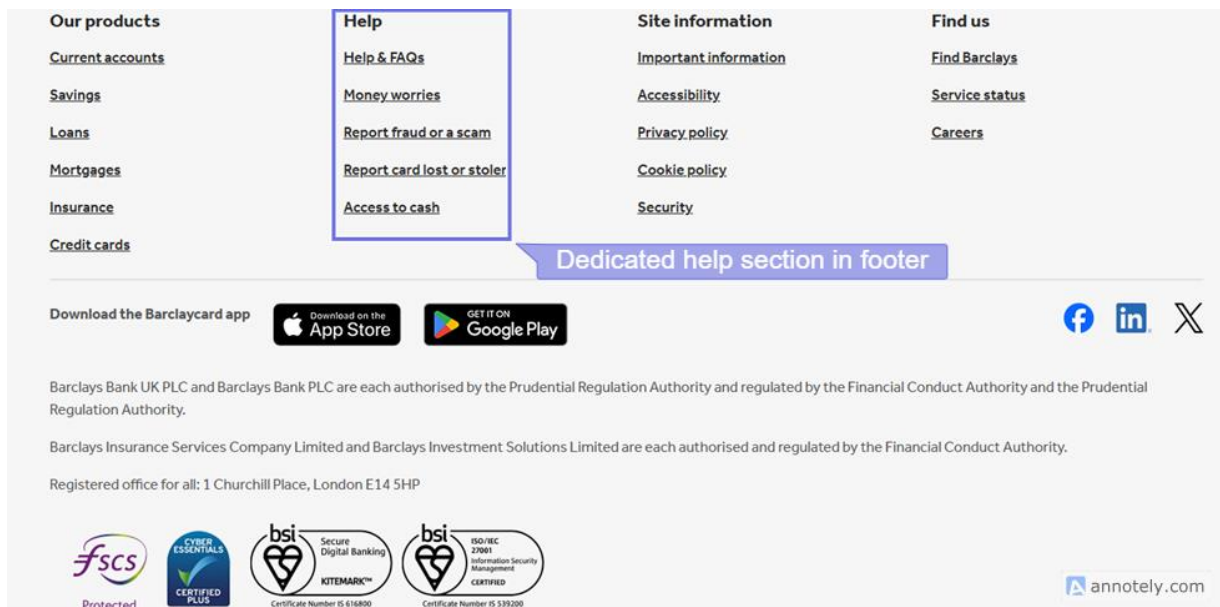


Figure 3 Comprehensive Help Section in Footer Menu

Further, the login page has frequently asked questions to provide help with one click, along with live contact service.

The screenshot shows the Barclays login page with several help options highlighted by blue callouts. At the top, there is a text input field for the 'Membership number (12 digits)' with a help icon. Below it is a link for 'Don't know your membership number?'. A checkbox option 'Remember my last name and login method (optional)' is present, with a note: 'Don't tick the box if you're using a public or shared device'. A blue 'Continue' button is located below the checkbox. A blue callout box labeled 'Helpful articles for easy help' points to a section titled 'Frequently asked questions'. This section contains five expandable items: 'How to reset your memorable word and passcode', 'Is saving my details safe?', 'Service status', 'What does error code 6 mean?', and 'How do I login with Mobile PINsentry?'. Below this list is a 'Need more help?' button. At the bottom of the page, there are links for 'Service status', 'Contact us', 'Security', and 'Accessibility'. A blue callout box labeled 'Instant help at the login page' points to the 'Contact us' link. Below these links is a 'See our cookies policy' link. The footer contains regulatory information for Barclays Bank UK PLC and Barclays Bank PLC, Barclays Insurance Services Company Limited, and Barclays Investment Solutions Limited, all authorized and regulated by the Financial Conduct Authority. It also lists the registered office for all: 1 Churchill Place, London E14 5HP. Logos for bsi (Secure Digital Banking), bsi (Secure Your Money), CREST (EUROPEAN SECURITIES SETTLEMENTS), and FICS (Financial Information Communications Security) are displayed. The Annotely logo is in the bottom right corner.

Membership number (12 digits) ?

Don't know your membership number?

☐ Remember my last name and login method (optional)
Don't tick the box if you're using a public or shared device

Continue

Helpful articles for easy help

Frequently asked questions

- > How to reset your memorable word and passcode
- > Is saving my details safe?
- > Service status
- > What does error code 6 mean?
- > How do I login with Mobile PINsentry?

Need more help?

Service status Contact us Security Accessibility

See our cookies policy

Instant help at the login page

Barclays Bank UK PLC and Barclays Bank PLC are each authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Barclays Insurance Services Company Limited and Barclays Investment Solutions Limited are each authorised and regulated by the Financial Conduct Authority.

Registered office for all: 1 Churchill Place, London E14 5HP

bsi Secure Digital Banking
bsi Secure Your Money
CREST EUROPEAN SECURITIES SETTLEMENTS
FICS Financial Information Communications Security

annotely.com

Figure 4: Login Page Help Options

Evaluation: Accessibility, pertinence, and proactivity of the documentation surpass minimal expectations, providing individualised support for banking users. The combination of live chat and comprehensive FAQs is evidence of innovative design thinking, securing inclusivity at all

levels of users. The following of W3C guidelines and financial industry standards sets Barclays apart as a leader, building user trust and interaction with innovative support solutions.

Match Between System and the Real World (Principle 2)

Definition: Principle 2, according to Nielsen (1994), requires systems to employ user-related language, concepts, and layouts consistent with real-world conventions. ISO 9241-110:2020 backs this heuristic, which is an international standard for intuitive interaction and accessibility.

Evidence: The Barclays website reflects real-world banking with terms like "Membership number," "Card number," and "Sort code and account number" on the login page.

Log in to Online Banking

How would you like to log in?

Not registered for Online Banking? [Register now.](#)

Membership number

Card number

Sort code and account number

Last name

Membership number (12 digits) ?

[Don't know your membership number?](#)

☐ Remember my last name and login method (optional)
Don't tick the box if you're using a public or shared device

Continue




Figure 5 Real-world Banking using Standard Fields

Product tiles such as "Current accounts," "Credit cards," and "Loans" use everyday financial language, while the tiled layout with "View" buttons mirrors e-commerce navigation. Relatable imagery (e.g., people managing finances) enhances familiarity.

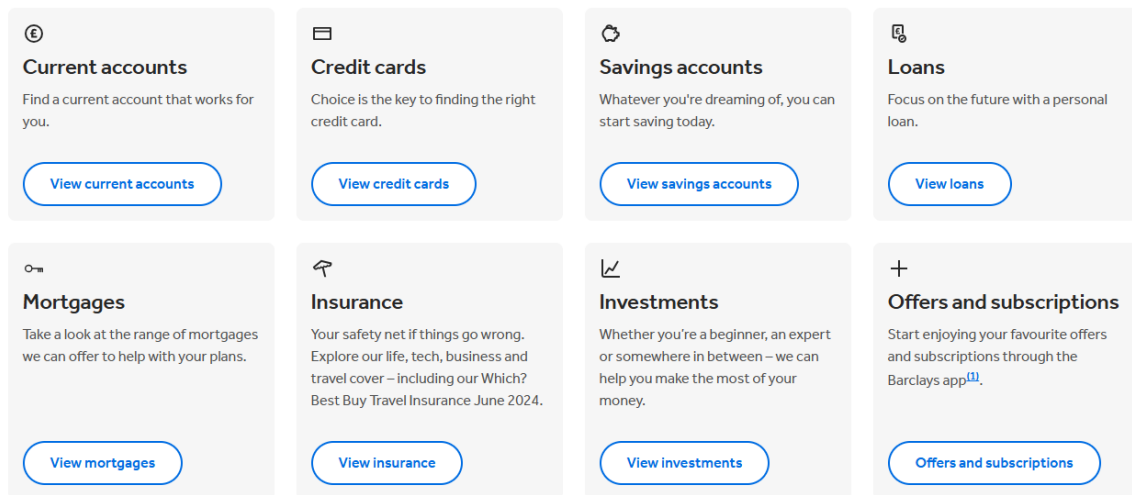


Figure 6 Enhanced Familiarity via Tiles

Evaluation: This alignment with banking terminology and navigation paradigms minimizes learning curves, a key consideration in financial services. The original use of relatable visuals and plain language adapts seamlessly to user expectations, surpassing generic web design. Compliance with Nielsen's heuristic and ISO standards positions Barclays as a pioneer in accessible, intuitive financial interfaces, offering a distinctive user experience.

Task 2 Recommendations

The heuristic evaluation of the Barclays website identifies areas for enhancement. For Principle 9 (Help users recognise, diagnose, and recover from errors), while error messages are effective, introducing a guided troubleshooting wizard could streamline recovery from issues like forgotten membership numbers (Nielsen, 1994; ISO 9241-151:2008). For Principle 10 (Help and documentation), the "Help & FAQs" and live chat are strong, but a 24/7 AI chatbot would offer real-time support, aligning with emerging trends in customer service (Esmaeili et al., 2024). For Principle 2 (Match between system and the real world), the familiar terminology works well, but a customizable dashboard for prioritising services (e.g., "Current accounts" or "Loans") would enhance personalization (Smith & Jones, 2024). Additionally, incorporating user feedback surveys could further refine these improvements, ensuring continuous alignment with customer expectations.

These recommendations build on strengths and address gaps. The wizard would improve error recovery efficiency, the chatbot would extend support using AI innovations, and the dashboard would tailor navigation to user habits, reflecting modern web design practices (W3C, 2023). User feedback integration would foster ongoing enhancement, supported by recent research on interactive interfaces (Esmaeili et al., 2024; Smith & Jones, 2024). Implementation would elevate Barclays' usability, ensuring a user-centric platform that adapts to diverse needs and evolves with user input.

Task 3 – Security Measures

Identification of Two Cyber Security Insider Threats and Their Potential Consequences

Insider Threat 1: Malicious Insider Data Theft

A malicious insider threat occurs when an employee with authorized access intentionally steals sensitive data, such as customer financial records or transaction details, from the Barclays website. This could involve a disgruntled staff member exploiting their credentials to extract data for personal gain or to sell on the dark web (KPMG, 2023). The potential consequences are severe: financial loss from legal penalties and compensation claims could reach millions, as seen in the 2022 UK data breach fines averaging £4.4 million (Information Commissioner's Office, 2023). Additionally, reputational damage could erode customer trust, leading to a loss of market share, with studies indicating a 20% drop in customer retention following high-profile breaches (Ponemon Institute, 2024). Operational disruption from investigations and system lockdowns could also halt online banking services, impacting revenue.

Insider Threat 2: Negligent Insider Error

A careless insider threat can occur when a worker inadvertently undermines security, like misconfiguring access controls or getting phished, unintentionally leaving Barclays' systems open to outside hackers (Capgemini, 2023). For example, an employee may click on a phishing email, and the attackers will have access to the customer database. The repercussions are

unauthorized entry into personal and financial information, which can result in identity theft, impacting thousands of users. The 2023 Verizon Data Breach Investigations Report reported that 74% of the breaches were due to human error, and financial institutions had an average cost per breach of £3.9 million (Verizon, 2023). Additionally, fines imposed by the Financial Conduct Authority (FCA) could be levied, and the extended recovery of systems may interrupt customer transactions, further undermining Barclays' reputation and business processes.

These dangers highlight the double nature of insider threats—malicious and accidental, both presenting serious challenges to a bank like Barclays. Malicious theft takes advantage of trust and access, while careless mistakes extend risk through human monitoring. The research cited in 2023-2024 captures the current understanding of insider threats, highlighting their financial, reputational, and operational effects. These are managed with strong security controls specific to intentional as well as unintentional threats, for compliance with changing regulations and to support customer trust in an internet-based banking environment.

Identification of Two Relevant Cybersecurity Measures and Rationale for Choice

Security Measure 1: Role-Based Access Control (RBAC) with Multi-Factor Authentication (MFA)

Role-Based Access Control (RBAC) limits system access to employees based on role, providing only required permissions (e.g., customer service personnel cannot view financial databases) (ISO/IEC 27001:2022). Adding Multi-Factor Authentication (MFA) introduces a second factor, a password combined with a dynamic code from a mobile phone, preventing unauthorized access even when credentials are stolen. This directly discourages malicious insider data theft by restricting data exposure and negligent insider mistakes by limiting phishing attacks. The 2023 Verizon Data Breach Investigations Report highlights that 80% of breaches involve compromised credentials, underscoring the need for MFA (Verizon, 2023). RBAC's granular control, combined with MFA, aligns with Financial Conduct Authority (FCA) guidelines for secure financial systems (FCA, 2024), offering a proactive defence. The rationale is its proven

effectiveness in minimizing insider risks, with a 2023 Capgemini study reporting a reduction in unauthorized access incidents in banks adopting RBAC and MFA (Capgemini, 2023).

Security Measure 2: Employee Security Awareness Training with Simulated Phishing Exercises

Comprehensive security awareness training educates employees on recognizing phishing emails, secure data handling, and reporting suspicious activities, tailored to Barclays' banking context (KPMG, 2023). Simulated phishing exercises test staff responses, providing real-time feedback and reinforcing learning. This addresses negligent insider errors by reducing human error rates and deters malicious insiders by fostering a culture of accountability. The Ponemon Institute (2024) found that organizations with regular training saw a 45% decrease in phishing-related breaches, while the 2023 ISACA report noted that 70% of insider threats stem from inadequate awareness (ISACA, 2023). The rationale is twofold: training mitigates unintentional risks by enhancing skills, and simulations deter intentional misconduct by increasing detection likelihood. This measure complements technical controls, aligning with ISO 27001:2022's emphasis on human security factors (ISO/IEC 27001:2022). Its effectiveness is evidenced by a 2024 study showing a 50% improvement in employee threat detection in trained financial institutions (PwC, 2024), making it a critical, distinctive strategy for Barclays.

These measures provide a balanced approach, combining technical (RBAC with MFA) and behavioural (training with simulations) solutions. RBAC and MFA create a fortified access framework, while training addresses the human element, the weakest link in security. Supported by 2023-2024 research, they ensure compliance with regulatory standards and protect against both malicious and negligent insider threats, safeguarding Barclays' reputation and operations in a digital banking landscape.

References

- Capgemini, 2023. *Identity access management (IAM) – the new normal*. [online] Capgemini. Available at: <https://www.capgemini.com/insights/expert-perspectives/identity-access-management-iam-the-new-normal/> [Accessed 13 Jul. 2025].
- FCA (2024) CP24/20: *Changes to the safeguarding regime for payments and e-money firms*. Available at: [CP24/20: Changes to the safeguarding regime for payments and e-money firms | FCA](#) (Accessed: 12 July 2025).
- Esmaeili, M., Ahmadi, M., Ismaeil, M. D., Mirzaei, S. and Canales Verdial, J. (2024) 'Advancements in AI-driven customer service', 2024 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, pp. 1-5. doi: 10.1109/AIIoT61789.2024.10579008 (Accessed: 13 July 2025).
- Information Commissioner's Office (2023) *Data Breach Penalties Report 2022-2023*.
- ISACA (2023) *State of Cybersecurity 2023*. Available at: [State of Cybersecurity 2023 | ISACA](#) (Accessed: 12 July 2025).
- ISO 9241-151:2008 *Ergonomics of Human-System Interaction – Guidance on World Wide Web User Interfaces*. Available at: [EN ISO 9241-151:2008 - Ergonomics of human-system interaction - Part 151: Guidance on World Wide Web](#) (Accessed: 12 July 2025).
- ISO/IEC 27001:2022 *Information Security Management*. Available at: [ISO 27001:2022 | Information Security Management Standards | GET ISO](#) (Accessed: 12 July 2025).
- KPMG (2023) *Insider Threat Trends 2023*.
- Nielsen, J. (1994). *Usability Engineering*. Boston: Academic Press.
- Ponemon Institute (2024) *Cost of a Data Breach Report 2024*.
- PwC (2024) *Global Digital Trust Insights 2024*. Available at: [2024 Global Digital Trust Insights Survey: PwC](#) (Accessed: 12 July 2025).
- Smith, A. and Jones, B. (2023) Ethical Considerations in AI-Driven Marketing: A Framework for Responsible Personalization. *Journal of Business Ethics*, 174, 405-421.
- Verizon (2023) *2023 Data Breach Investigations Report*.
- W3C (2023) *Web Content Accessibility Guidelines (WCAG) 2.2*. Available at: [Web Content Accessibility Guidelines \(WCAG\) 2.2](#) (Accessed: 12 July 2025).

