資訊專案文件與開源碼詮釋資料中文化
第四項
使用 CAPTCHAs

執行單位：國家資通安全研究院
中華民國 112 年 9 月

使用 CAPTCHAs

CAPTCHAs 是用來測試和區分人類和機器人(例如：自動化軟體)的工具，藉由讓使用者執行特定任務來證明自己是人類 - 例如，送出表單前先辨識混淆過的文字並輸入結果。
CAPTCHAs 影響了安全、隱私、可用性和無障礙等議題。除非運用於下列場合，否則切勿使用：

- 用於偵測可疑活動(例如，限制在用於偵測到可疑行為，並且需要測試使用者是否為人類)
- 有證據顯示替代方案不適用

CAPTCHAs are used to try and distinguish between humans and bots automated software). They do this by having users perform a task to prove they're human - for example, decipher and enter jumbled up text before submitting a form.
There are security, privacy, usability and accessibility issues associated with CAPTCHAs. You must not use them unless you both:

- limit their use to cases where you detect suspicious activity for example, you detect bot-like behaviour and need to test whether the user is human)
- have evidence to show that alternative solutions will not work for your service
  Why CAPTCHAs are problematic

為什麼 CAPTCHAs 造成問題

CAPTCHAs 會讓部分的人較難使用我們的服務，含身心障礙者。第三方的 CAPTCHA 服務也會帶來額外風險，含：

- 資安問題 - 如果 CAPTCHAs 的提供方安全受損，我們的服務也會收到影響
- 隱私疑慮 - 例如，第三方服務可設定 cookies，收集分析資料並跨站追蹤使用者
- 效能問題 - 如果我們依賴 CAPTCHAs 提供者，代表我們將受到第三方會遇到的效能問題或斷線影響
- 即使具備 CAPTCHA 機制，我們的服務仍然可能面臨風險。透過電腦影像技術的進步或使用 CAPTCHA 農場 CAPTCHA farms) 進行破解，使得仍有某些機器人得以存取我們的服務。

Why CAPTCHAs are problematic

CAPTCHAs will make your service more difficult for some people to use, including disabled people.
Third-party CAPTCHA services could also introduce additional risks, including:

- security issues - if your provider's security is compromised, your service and its users may also be affected
- privacy concerns - for example, third-party services might set cookies, collect analytics and track users across multiple sites
- performance issues - if you rely on a supplier, it means you'll be affected by any performance problems or outages they experience

Your service could still be at risk, even with a CAPTCHA in place. Advances in computer imaging and the use of CAPTCHA farms means some bots will still be able to access your service.

CAPTCHAs 的替代方案

許多 CAPTCHAs 所設計用來降低的風險，也可以透過其他方式來達到，含：

- 控制造訪速率和連線數
- 運用蜜罐誘捕系統 (honey pots)
- 監控資料交換動態

您也可以和前端社群一起討論關於 CAPTCHAs 的其他可能方案。.

Alternatives to CAPTCHAs

Many of the risks that CAPTCHAs are aimed at reducing can be addressed in other ways including:

- rate and connection limiting
- using honey pots
- transaction monitoring

You can discuss alternatives to CAPTCHAs with the frontend community.

相關指南

您可能會發現以下指南也很有用：

- 保護您的服務免受詐騙的指南
- 使用 cookies 和類似技術的工作指南

Related guides

You may also find the following guides useful:

- Protecting your service against fraud
- Working with cookies and similar technologies

相關翻譯
監控交易動態
監控您服務的狀態
https://www.gov.uk/service-manual/technology/monitoring-the-status-of-your-service

當您進入公開 beta 測試階段時，您必須建立監控機制，以識別可能影響您服務的任何問題。
使用適當的工具和流程進行監控可以幫助您：

- 發現使用者可能遇到的問題
- 在技術問題發生時收到警報，以便及時修復
- 在問題發生或加劇之前預見問題
- 改進您的服務，例如使用效能數據來協助容量規劃等。

Monitoring the status of your service
By the time you reach public beta, you must have monitoring in place for your service to identify any problems that might affect it.
Monitoring with the right tools and processes allows you to:

- discover any problems that users have
- get alerts when technical problems occur so you can fix them
- anticipate problems before they happen or become more serious
- improve your service, for example by using performance data to help with capacity planning

規劃您的監控工作

您應該在 alpha 階段開始規劃如何監控您的服務。在 alpha 階段，您的團隊應該達成以下協議：

- 監控服務的哪些部分
- 如何監控您的服務
- 如何處理和記錄問題

Plan your monitoring

You should start planning how to monitor your service during alpha.
During alpha, your team should agree:

- what to monitor in your service
- how to monitor your service
- how to process and record issues

監控指標

您應該追蹤使用者相關的指標，以及技術性的指標。例如，追蹤能夠完成任務的使用者百分比，以及可用的硬碟空間、應用程式介面(API)效能和記憶體使用情況。

Metrics to monitor

You must track user-related metrics, as well as technical metrics. For example, track the percentage of users that can complete a task as well as available disk space, application programming interface API) performance and memory usage.

如何進行監控

一旦您同意監控的內容，您的團隊應該：

- 設定內部和外部的監控檢查(monitoring checks)
- 撰寫監控檢查
- 撰寫警報訊息

How to monitor

Once you've agreed what to monitor, your team should:

- set up internal and external monitoring checks
- write monitoring checks
- write alerts

設定內部和外部監控檢查

您應該設定內部和外部的監控檢查。
內部監控是您應該在您的基礎架構內設定的監控，提供關於記憶體使用量、頁面載入時間和網路流量等指標的即時更新。
外部監控是您應該在您的服務外設定的監控，即使您的基礎架構發生故障，它仍會持續檢查您的系統。

Setting up internal and external monitoring checks

You should set up internal and external monitoring checks.
Internal monitoring is the monitoring you should set up inside your infrastructure and will give you realtime updates about metrics like memory usage, page load times, and network traffic.
External monitoring is the monitoring you should set up outside of your service which keeps checking your systems even if your infrastructure goes down.

撰寫監控檢查

您需要決定哪種監控檢查對您的服務最有用。
監控檢查是一系列測試，您可以執行這些測試來評估您的系統或整體服務的狀態，並通知您是否存在問題。
例如，您可能決定「如果在一小時內有 1%的使用者在完成交換資料時遇到問題，則需要收到警報」。

您應該在撰寫程式碼的同時撰寫監控檢查，並將這些檢查視為您實際系統的測試。

Writing monitoring checks

You need to decide the type of monitoring checks that are most useful to your service.
A monitoring check is a series of tests that you can run against your systems or overall service to assess their status and tell you if something is wrong.
For example, you might decide you need to see an alert if 1% of users in an hour have problems finishing a transaction.
You should write monitoring checks at the same time as writing code and treat your checks as tests for your live system.

撰寫警報訊息

請確保您的警報訊息清晰簡潔，易於理解，因為可能會有團隊成員在夜間被叫醒來解決問題。
考慮建立一份作業手冊或文件，以幫助您的團隊快速應對問題。請確保團隊的每個成員在本機上都有檔案的副本，以防雲端文件儲存空間不可用的情況。

Writing alerts
Make your alert messages clear and concise. They need to be easy to understand for team members who might be woken up in the night to fix a problem.
Consider creating an operations manual or documentation to help your team deal with problems quickly. Make sure every member of your team has a local copy of the documentation in case your cloud-based documentation storage is unavailable.

處理和記錄問題
您應該使用報修單追蹤系統(ticketing system)來管理和追蹤錯誤，以便讓您將問題分配給團隊成員。
錯誤訊息總是包含有用的資訊——它們可以告訴您以下內容：

- 使用者問題
- 對服務的攻擊
- 系統故障
- 容量問題

追蹤錯誤有助於您查看哪些錯誤是重複出現的，以及它們是整體服務的一部分還是與特定應用程式或機器相關。

您可以結合監控測試結果以更了解服務中應修復的問題。例如，比對頁面載入測試中的資料交換失敗和應用程式錯誤，可以讓您：

- 找出更多使用者在服務中遭遇問題的部分
- 確定問題的原因
- 討論如何解決問題的根本原因，例如硬碟空間或效能不佳。

Processing and recording issues
You should manage and track errors using a ticketing system that allows you to delegate them to members of your team.
Errors always contain interesting information - they can tell you about:

- a user problem
- attacks on your service
- failing systems
- problems with capacity

Tracking errors helps you to see which ones are recurring and whether they’re part of the overall service or related to a particular application or machine.
You can combine monitoring test results to better understand what to fix in your service. For example, comparing page-loading tests with failed transactions and application errors allows you to:

- find out the parts of your service where more users are having problems
- identify the cause of problems
- discuss how to fix the cause of problems, for example, disk space or slow performance

讓資料可以被廣泛利用
除非有安全性問題，您應該將監控資訊和資料廣泛分享。

例如，您可以與您部門的其他服務團隊分享效能報告，或使用類似 GOV.UK Notify 所使用的作業狀態頁面的狀態儀表板，來告訴使用者問題資訊。

Make data widely available

Unless it's not safe to do so, you should make monitoring information and data widely available.

For example, you can share performance reports with other service teams in your department or use a status dashboard, like the operations status page used by GOV.UK Notify, to tell users about any issues.

定期檢視您的監控流程

每次收到警報時，您都應該檢視您的監控流程。

如果有人在非工作時間被呼叫，您應該確保問題確實需要相應等級的的回應。

例如，如果該問題不影響使用者，並且可以等到早上再處理，請考慮更改您的警報策略，以便將來不再對此類錯誤發出警報。

Reviewing your monitoring processes regularly

You should review your monitoring processes every time you get an alert.

If someone is called out of hours, you should make sure the issue needed that level of response.

For example, if the issue didn't affect users and could have waited until the morning, consider changing your alert strategy so that type of error doesn't prompt an alert in future.

相關指南

您可能也會發現「運作時間和可用性指南」很有用。

Related guides

You may also find the Uptime and availability guide useful.

相關翻譯

保護您的服務免受詐騙的指南

保護您的服務免受詐騙

https://www.gov.uk/service-manual/technology/protecting-your-service-against-fraud

當您設計和管理您的數位服務時，您必須：

- 考慮您的服務如何成為詐騙份子的目標(從 Alpha 階段開始)，以及這可能會造成的影響
- 儘量保護您的使用者和您的服務免於詐騙的侵害
- 本指南涵蓋詐騙的基本知識。如果您需要更多資訊，請與以下人員聯繫：
- 如果您的組織中有反詐騙專家，請與他們聯絡
- 如果您的組織中沒有專家，請聯繫內閣辦公室的反詐騙專職部門

Protecting your service against fraud

When you're designing and managing your digital service, you must:

- consider how it could be targeted by fraudsters start at the alpha stage) and the impact this could have
- protect your users and your service as much as possible from fraud

This guide covers the basics of fraud. If you need to know more, talk to:

- a counter fraud expert in your organisation, if there is one
- the Counter Fraud Function in the Cabinet Office, if there's no expert in your organisation

詐騙類型

以線上服務為目標的詐騙份子通常會嘗試：

- 從服務中獲取金錢
- 假裝他們有資格使用服務
- 獲取資訊再針對其他服務
- 利用服務進行洗錢

一些詐騙類型比其他類型更嚴重。例如，高階詐騙是有組織的犯罪份子以多種服務為目標來騙取金錢。低階詐騙可能是您的一名員工利用系統中的漏洞來獲利。

一些小規模詐騙可能會在您的服務或組織之外導致更嚴重後果。例如，如果有人偽造某個服務，他們可能會利用這個假資格來詐騙另一個服務。

Types of fraud

Fraudsters that target online services usually try to:

- take money from a service
- pretend they're eligible for a service
- extract information to target other services
- use a service for money laundering

Some types of fraud are more severe than others. For example, high-level fraud would be organised criminals targeting multiple services to get money. Lower-level fraud could be one member of your staff taking advantage of a vulnerability in a system.

Some small-scale fraud may lead to more serious consequences beyond your service or organisation. For example, if someone faked a claim for one service, they could use that fake

eligibility to defraud another service.

注意到線上服務的弱點

如果您將離線服務轉移到線上，您應該注意在此過程中可能　　的新弱點。

線上服務更容易受到詐騙的攻擊，詐騙份子可以在短時間內多次嘗試。

當服務轉移到線上時，不要假設您在離線情況下遵循的任何安全流程可以完全保護您的服務免受詐騙的威脅。

Consider the weaknesses of online services

If you're moving an offline service online, you should consider any new weaknesses that may be introduced in the process.

Online services are more open to fraud and fraudsters can try multiple attempts in a short space of time.

Do not assume any security processes you're following offline will fully protect your service from fraud when the service moves online.

考慮非金融詐騙

即使您的服務不向使用者支付費用，詐騙份子仍可能試圖攻擊該服務以獲得資訊，然後使用這些資訊進行詐騙。

例如，他們可能利用使用者的個人資訊以便從其他政府服務、民營部門或個人中獲取金錢或其他好處。

Consider non-financial fraud

Even if your service does not pay out money to users, fraudsters may still try to attack it to get information which they could use to commit fraud.

For example, they could use your users' personal details to access money or other benefits from other government services, the private sector or individuals.

保護您的服務免受詐騙

依照以下步驟來保護您的服務免受詐騙。

1. 分析風險。
2. 降低風險。
3. 應對不斷變化的威脅。
4. 將資訊與獨立來源進行核對。
5. 讓您的團隊認知詐騙風險。

Protecting your service against fraud

Follow these steps to protect your service against fraud.

1. Analyse the risk.
2. Reduce the risk.
3. Respond to changing threats.
4. Check information against independent sources.
5. Make your team aware of fraud risks.

評估風險

您必須在您的服務 Alpha 階段開始考慮詐騙風險。

檢查是否已完成初始詐騙影響評估(Initial Fraud Impact Assessment, IFIA)或完整詐騙風險評估(Full Fraud Risk Assessment, FRA)。

IFIA 概述詐騙可能影響政策、專案或計畫的主要方式。

完整的 FRA 是針對特定流程和計畫的深入風險評估。它解釋了現有控制措施如何降低風險以及賸餘的弱點為何。

如果您沒有 IFIA 或完整的 FRA，請聯繫反詐騙專家。

當您建立第一個原型時，您應該檢查服務的潛在風險區域，這些區域可能會讓詐騙份子有機可乘。

例如，著重於關注那些需要使用者分享個人資訊的部分。小工具(Widgets)或表單可能會要求使用者提供詐騙份子感興趣的資訊，尤其是使用者被提示要更改地址或銀行資訊。

一旦您了解了您的服務如何收集敏感資訊，請檢查個人或系統如何儲存、傳輸或存取這些資料。

Assess the risk

You must start considering fraud risks during your service's alpha phase.
Check if an Initial Fraud Impact Assessment IFIA) or a Full Fraud Risk Assessment FRA) has been completed.
An IFIA gives an overview of some of the main ways fraud could affect a policy, project or programme.
A Full FRA is a thorough assessment of the risks within specific processes and programmes. It explains how the controls in place reduce them and what the remaining vulnerabilities are.
If you do not have an IFIA or Full FRA, contact a counter fraud expert.
As you build your first prototypes, you should review the potential areas of your service that could be left vulnerable to fraud.
For example, focus on parts of your service where users have to share personal information. Widgets or forms may ask users for information that's attractive to fraudsters, particularly if a user is prompted to change their address or bank details.
Once you've found how your service gathers sensitive information, check how individuals or systems store, transport or access this data.

降低風險

您必須試圖降低您已識別的詐騙風險。使用您的 IFIA 或完整的 FRA 來支援您降低風險的方法。

降低這些風險的方式取決於您的服務以及可能受到影響的詐騙類型。

例如，如果您的服務只向英國使用者開放，您可以建立一個系統來檢查任何非英國的請求並詳細審查這些請求。

如果您知道某些支付機制具有更高的詐騙率，您可能得將它們視為較高風險。

您還可以檢查使用者的瀏覽器和 IP 地址是否與其常用的瀏覽器和 IP 地址匹配。突然的變化可能是詐騙活動的跡象，您可能希望將它們視為較高風險。

您無需因瀏覽器或 IP 地址的更改而自動阻止資料交換。根據您的服務及其功能，您可以延遲或記錄它們，或要求其他形式的驗證來處理請求。

Reduce the risk

You must attempt to reduce the fraud risks that you've identified. Use your IFIA or Full FRA to support your approach to risk mitigation.
The way to reduce these risks depends on your service and the type of fraud that it could be affected by.
For example, if your service is only open to UK users, you could set up a system to check any non-UK requests and review them in detail.
If you know that certain payment mechanisms have higher fraud rates, you might treat them as higher risk.
You could also check that a user's browser and IP address matches their usual browser and IP address. Sudden changes might be a sign of fraudulent activity and you may wish to treat them as higher risk.
You do not need to automatically prevent a transaction because of a change in browser or IP address. Depending on your service and what it does, you could delay or record it, or require other forms of verification to process the request.

預防身分詐騙

由於詐騙份子在網路上分享被盜的個人資料，導致身分盜竊和詐騙問題日益嚴重。為了保護您的使用者，請遵循有關如何證明和驗證某人身分的指南。這些指南說明瞭如何檢查客戶、員工或企業代表的身分。

Preventing identity fraud

Identity theft and fraud are growing problems with fraudsters sharing stolen personal details online. To protect your users, follow guidance on how to prove and verify someone's identity. This sets out how to check the identity of a customer, an employee or someone acting on behalf of a business.

應對不斷變化的威脅

詐騙份子經常改變其詐騙企圖的性質和頻率，因此請確保您的服務足夠靈活，能夠應對不斷變化的威脅。

例如，如果您設定限制詐騙活動的規則，請確保您可以容易更改這些規則，而且它們沒有寫死 hard-baked)在系統中。

您的組織可能會使用安全分類來標記安全風險。如果將這些分類應用於詐騙企圖(fraud attempt)，請確保可以根據新出現的威脅嚴重性來更改它們。

Respond to changing threats

Fraudsters regularly change the nature and frequency of their fraud attempts, so make sure your service is flexible enough to respond to changing threats.
For example, if you've set rules to limit fraudulent activity, make sure you can change them easily and that they aren't 'hard-baked' into your system.
Your organisation may use security classifications to label security risks. If you apply these

classifications to fraud attempts, make sure you can change them according to the severity of new threats that appear.

核查使用者資訊是否與獨立資料來源相符

您應該將使用者提供的資訊與權威清單進行核對。例如，您可以參考授權銀行的帳戶、地址和其他個人資料的清單，以識別任何虛假資訊。

請注意，並非每個不正確的輸入都代表詐騙活動。當您與可靠和獨立的來源進行核對時，您應該考慮使用者可能會真的犯錯。

Check user information against independent sources

You should check the information users give you against authoritative lists. For example, you can reference lists of authorised bank accounts, addresses and other personal details to identify any false information.

Be aware that not every incorrect entry means fraudulent activity. Users can make genuine errors and you should take these into account when checking against reliable and independent sources.

讓團隊認知詐騙風險

您必須確保團隊中的每位成員都了解詐騙對服務所構成的風險，以免因錯誤而產生弱點。

在設計和維護您的服務時，定期與反詐騙專家進行對談，以幫助降低詐騙的風險和影響。

Make your team aware of fraud risks

You must make sure every member of your team understands the risk of fraud to your service so that they don’t add vulnerabilities by mistake.

While designing and maintaining your service, talk to counter fraud experts regularly to help reduce the risk and impact of fraud.

監控您的服務以防詐騙

監控您的服務是否有可疑行為，幫助您識別詐騙活動。

您可以使用「資料交換(transaction)監控系統」來追蹤使用者行為並發現可疑活動。

利用您找到的資訊來：

- 檢測詐騙，阻止詐騙份子存取您的服務
- 在詐騙活動完成後識別詐騙活動
- 追蹤詐騙份子，並採取適當的行動，如追回被詐騙索取的款項或法律訴訟。

Monitoring your service for fraud

Monitor your service for suspicious behaviour to help you identify fraudulent activity.

You can use ‘transaction monitoring systems’ to track user behaviour and spot suspicious activity.

Use the information you find to:

- detect fraud stop fraudsters from accessing your service
- identify fraudulent activity after it’s been completed

- trace fraudsters and take appropriate action such as recovering money that has been fraudulently claimed or legal action

保留詐騙活動紀錄

在您的安全和風險紀錄中記錄所有的詐騙嘗試。記錄試圖詐騙的時間、日期和試圖的類型，以及是否成功。

詐騙份子通常會嘗試詐騙，改變策略，然後再次嘗試。在可能的情況下，您應該與其他政府機構和部門分享有關詐騙企圖的資訊，以提高警覺。

網路安全資訊共享合作夥伴關係(Cyber-security Information Sharing Partnership)可以幫助您與其他人交換此資訊。如果您不確定分享關於詐騙企圖的資訊是否安全，請諮詢您的反詐騙專家。

Keep a record of fraudulent activity

Keep track of all fraud attempts alongside your security and risk log. Note the time, date and type of attempt as well as whether it was successful.
Fraudsters will often try to commit fraud, change tactics and try again. Wherever possible, you should share information about fraud attempts with other government agencies and departments to raise awareness.
The Cyber-security Information Sharing Partnership can help you exchange this information with others. Check with your counter fraud expert if you are unsure if it's safe to share information about fraud attempts.

進一步閱讀

您可能會發現以下指南有所幫助：

- 國家網路安全中心關於安全開發和部署的指南
- 政府詐騙風險評估的專業標準和指南

Further reading

You might find this guidance useful:

- National Cyber Security Centre guidance on secure development and deployment
- Professional standards and guidance for fraud risk assessment in government

相關指引

您可能會發現以下指南有所幫助：

- 資通安全
- 雲端安全

Related guides

You may also find these guides useful:

- Information security
- Cloud security

相關翻譯

使用 cookies 和類似技術的工作指南

使用 Cookie 和類似技術

https://www.gov.uk/service-manual/technology/working-with-cookies-and-similar-technologies

Cookie 是網站發送到使用者電腦的小型資料檔，用於儲存有關使用者瀏覽網站的資料。

本指南是介紹如何使用 Cookie，但當採用使用者設備中其他資訊儲存的技術時，您應該遵循相同的指南，例如 HTML5 local storage。

Working with cookies and similar technologies

Cookies are small data files that a website sends to a user's computer. They're used to store information about how users browse a website.

This guidance is about how to use cookies, but you should also follow it when using any other technologies that store information on a user's device, like HTML5 local storage.

如何使用 Cookie

儘量減少 Cookie 的使用，並對您使用的 Cookie 透明化。您必須：

- 盡可能使用少量 Cookie，停用任何不再需要的 Cookie
- 儘量儲存所需的最少量資訊，並盡可能縮短保存時間
- 發布 Cookie 政策，告知使用者使用了哪些 Cookie
- 在設定任何對您所提供服務非必要的 Cookie 前，必須要獲得使用者的同意

How to use cookies

Keep use of cookies to a minimum, and be transparent about the ones you do use. You must:

- use as few cookies as possible, and stop setting any cookies that are not needed anymore
- store the smallest amount of information that you need, for as short a time as necessary
- publish a cookie policy telling users about the cookies you're using
- get users' consent before you set any cookies that are not essential to providing the service

如何建立 Cookie 頁面

在 GOV.UK 設計系統中提供了以下相關資訊：

- 如何建立 cookie 頁面，含哪些 Cookie 需要徵得同意
- 如何建立 Cookie 標題

How to create a cookies page

There's information on the GOV.UK Design System about:

- how to create a cookies page including which cookies you need consent for
- how to create a cookie banner

應用 Cookie 的範圍

Cookie 必須僅適用於您的原始網域。例如，www.servicename.service.gov.uk 而非.gov.uk。

不要在僅托管靜態資源(詳見圖像或 JavaScript)的網域上使用 Cookie——它只會降低使用者的回應時間，並且沒有任何好處。

您應該只發送帶有 Secure 屬性且在適當情況下帶有 HttpOnly 屬性的 Cookie。這些旗標(flag)提供瀏覽器如何處理 Cookie 提供的額外保證。

Where to apply cookies

Cookies must only apply to your originating domain name. For example, www.servicename.service.gov.uk not .gov.uk.

Do not use cookies on domains that host only static assets like images or JavaScript - they slow response times for users without providing any benefit.

You should only send cookies with the Secure attribute and, when appropriate, the HttpOnly attribute. These flags provide additional assurances about how browsers should handle cookies.

相關指南

您可能會發現有關選擇數位分析工具的指南很有用。

Related guides

You might find the guidance on choosing digital analytics tools useful.