# O incidente do Portal das Finanças e o estado da cibersegurança em Portugal

Público · 2024-10-23




---

*Está na altura de refletirmos a fundo sobre o papel de cada um na construção de um ecossistema digital mais seguro*

---

---

file: 2024-10-23-publico-incidente-portal-financas-estado-ciberseguranca-portugal.md

title: O incidente do Portal das Finanças e o estado da cibersegurança em Portugal

outlet: Público

date: 2024-10-23

date_display: "23 de outubro de 2024, 19:05 (Europe/Lisbon)"

url: "https://www.publico.pt/2024/10/23/opiniao/opiniao/incidente-portal-financas-estado-ciberseguranca-portugal-2109190"

author_page: "https://www.publico.pt/autor/joao-luis"

byline: João Luís

affiliation: Especialista em cibersegurança na Dashlane

text_status: full

section: Opinião

extract: publico

word_count: 926

---

# O incidente do Portal das Finanças e o estado da cibersegurança em Portugal

*João Luís, Especialista em cibersegurança na Dashlane*

*Público, 23 de outubro de 2024, 19:05 (Europe/Lisbon)*

*https://www.publico.pt/2024/10/23/opiniao/opiniao/incidente-portal-financas-estado-ciberseguranca-portugal-2109190*

Apenas alguns dias após o ciberataque de ransomware à Agência para a Modernização Administrativa (AMA), chegou ao conhecimento público uma nova violação de segurança. Em agosto, milhares de credenciais de utilizadores do Portal das Finanças foram divulgadas na internet, revelando uma falha crítica na

salvaguarda dos dados dos cidadãos nacionais. Foi exposta uma lista com 15 mil entradas, dando-se como certo que pelo menos nove mil corresponderão a dados de acesso reais.

Sabendo-se que os dois incidentes não estão diretamente relacionados, os motivos que levaram à exposição destas credenciais ainda não são totalmente claros, acreditando-se que estas terão sido comprometidas graças a vulnerabilidades nos dispositivos dos próprios utilizadores ou em sistemas de terceiros. Ainda assim, uma exposição desta natureza sugere que a AT - Autoridade Tributária e Aduaneira não implementou medidas suficientemente robustas de cibersegurança, essenciais para a proteção de dados altamente sensíveis.

A responsabilidade das entidades públicas nestes casos é inegável. Como responsáveis pelas identidades digitais dos cidadãos, cabe-lhes assegurar que são aplicadas as melhores práticas de segurança, contemplando não só os sistemas sob a sua gestão direta, mas também a fiscalização rigorosa de sistemas de terceiros que possam interagir com os seus. Não é aceitável que o acesso a um portal essencial do Estado ainda disponibilize um método de autenticação composto simplesmente por um username e uma password (o mesmo acontece, aliás, com o portal da Segurança Social Direta).

Os impactos deste acontecimento podem comprometer a segurança dos cidadãos a vários níveis. Desde logo, a exposição das identidades digitais deixa-os sujeitos a potenciais crimes financeiros e de fraude fiscal, como roubo de identidade, submissão de declarações fraudulentas ou desvio de reembolsos. De forma mais indireta, é afetada a confiança das pessoas nos sistemas públicos e no Estado. Tal pode desencadear uma desconfiança generalizada em relação à digitalização dos serviços públicos, travando as tão necessárias iniciativas de modernização digital. Por fim, não nos podemos esquecer das consequências legais, uma vez que a violação do Regulamento Geral sobre a Proteção de Dados (RGPD) pode trazer multas pesadas e processos judiciais contra o Estado.

Após o incidente se ter tornado do domínio público – e sem qualquer comunicação prévia aos utilizadores ou explicação oficial acerca do sucedido –, a AT anunciou a revogação das passwords afetadas, mas esta é uma medida que se revela manifestamente insuficiente. De forma transversal, mas principalmente em plataformas que contêm informações pessoais críticas, é imperativa a adoção imediata de mecanismos mais seguros em paralelo com as passwords e que adicionem um patamar extra de segurança, como sistemas de autenticação multifator. Também a monitorização eficaz e proativa de todas as contas associadas ao Portal é essencial, no sentido de identificar acessos suspeitos ou comportamentos incomuns, assim como o reforço da segurança dos sistemas que interagem com a AT, garantindo o cumprimento dos padrões exigidos de segurança por parte de terceiros.

Considerar uma auditoria completa de segurança para identificar eventuais vulnerabilidades adicionais é outra medida que se impõe, garantindo transparência total na apresentação de resultados. Por fim, a entidade deveria notificar diretamente e proativamente todos os utilizadores acerca da necessidade de reforçarem a segurança das suas contas, incluindo conselhos sobre como proteger melhor os seus dispositivos contra malware e phishing e sobre como aumentar a segurança das suas passwords, enquanto mecanismos mais robustos não são implementados.

Sendo indiscutível que cabe às entidades públicas fornecer sistemas seguros, é também claro que os utilizadores têm um importante papel na sua própria proteção. Infelizmente, esta falha mostrou-nos que a segurança das passwords ainda é, em muitos casos, inadequada, como é possível verificar pelas passwords divulgadas. Utilizar o nome próprio, o número de contribuinte, ou simplesmente “123456” ou “password” como credencial de acesso a um Portal desta relevância revela a necessidade de uma maior sensibilização e educação acerca dos riscos e consequências associados a incidentes deste género.

Utilizar o nome próprio, o número de contribuinte, ou simplesmente '123456' ou 'password' como credencial de acesso a um Portal desta relevância revela a necessidade de uma maior sensibilização e educação acerca dos riscos e

consequências associados a incidentes deste género

Partilhar citação

Partilhar no Facebook

Partilhar no Twitter

Sabemos que muitas violações de segurança acontecem devido a erros humanos, como desconhecimento sobre phishing, falta de atualização de software ou utilização de passwords fracas e/ou repetidas. Gerar passwords longas, complexas e evitar a sua reutilização, através de uma aplicação de gestão de identidade digital, é uma das formas mais eficazes de garantir a salvaguarda de informações pessoais e deveria já ser prática comum e transversal.

Mesmo com sistemas altamente protegidos, se o utilizador não adotar práticas essenciais de segurança, ficará igualmente vulnerável a ataques. E aqui entra a importância de discutirmos verdadeiramente a transição para um futuro passwordless, com a envolvência e colaboração entre diversos atores. A adoção de passkeys de forma mais comum e massificada – fazendo com que a proteção dos dados pessoais deixe de depender da interação humana e seja garantida pelo sistema do dispositivo que está a ser utilizado – é mesmo a única forma de retirar grande parte dessa responsabilidade que ainda recai sobre o utilizador, minimizando vulnerabilidades.

Que este incidente inspire uma maior transparência por parte das entidades públicas e sirva como um alerta claro e decisivo para a necessidade urgente de reforço das práticas essenciais de segurança, tanto a nível institucional como individual. Está na altura de refletirmos a fundo sobre o papel de cada um na construção de um ecossistema digital mais seguro e na definição de um novo paradigma para a cibersegurança em Portugal.

O autor escreve segundo o novo acordo ortográfico