bilingue edition

ptsoc{news}

0 fim das pa55w0rdS.

3 perguntas a Cristina Almeida

Autenticação de dois fatores (2FA)
por José Ramos

05

Pa55w0rds are out.

3 questions to Cristina Almeida

Two-factor authentication (2FA)
by José Ramos

.pt

O fim das *pa55w0rdS*. Vêm aí as passkeys.

O número dos defensores de que as passwords, ou palavras-chave, já não satisfazem o fim para o qual foram idealizadas tem aumentado. É o seu fim que está agora em causa. Mas o desaparecimento não será total e elas podem apenas vir a ser substituídas em breve pela norma FIDO (de Fast IDentity Online).

As passwords surgiram no início da década de 1960 após um professor do MIT, Fernando Corbató, desenvolver um protótipo do Compatible Time-Sharing System (CTSS), com Marjorie Daggett e Bob Daley. Este sistema partilhado ("time-share") usava "um pequeno sistema operativo que geria quatro máquinas de escrever. O armazenamento de backup foi obtido atribuindo uma unidade de fita magnética a cada máquina de escrever".

Corbató queria "um novo tipo de sistema de computador partilhado e uma maneira de as pessoas protegerem os seus ficheiros privados. A solução foi uma password. Ao longo dos anos, a opção de Corbató triunfou sobre outros meios de autenticação e tornou-se o modo normal para nos ligarmos em praticamente tudo, em todos os lugares".

Este triunfo não é pacífico. A par com a "força bruta" que pode ser usada em sis-

Pa55w0rds are out. Passkeys are in.

The number of advocates that passwords, or keywords, no longer satisfy the end for which they were intended has increased. It is their end that is now at stake. But they will not disappear altogether, they can just soon be replaced by the FIDO (Fast IDentity Online) standard.

Passwords emerged in the early 1960s after an MIT professor, Fernando Corbató, developed a prototype of the Compatible Time-Sharing System (CTSS) with Marjorie Daggett and Bob Daley. This time-share used 'a small operating system that ran four typewriters. Backup storage was obtained by assigning a magnetic tape drive to each typewriter'.

Corbató wanted 'a new kind of shared computer system and wanted a way for people to be able to protect their private files. His solution was a password. Over the years, Corbató's fix won out over other means of authentication and

temas informáticos para as desvendar, elas podem ser roubadas, adivinhadas e mal escolhidas pelos utilizadores, e até armazenadas em gestores de passwords, enfrentando o perigo de as colocar todas no mesmo local.

Em resumo, defendem muitos, é preciso mudar o paradigma da cibersegurança assente em palavras de dicionários, reinventá-las ou acabar mesmo com as passwords tal como as conhecemos.

Até mesmo o autor das regras mais rígidas para as passwords concedeu há cinco anos que se chegou a um ponto irreversível, expresso no título de um artigo no The Wall Street Journal: "The Man

became the standard way we log on to pretty much everything, everywhere.'

This triumph is not peaceful. Along with the 'brute force' that can be used in computer systems to figure them out, they can be stolen, guessed and poorly chosen by users, and even stored in password managers, facing the danger of putting them all in the same place.

In short, many defend, we need to change the paradigm of cybersecurity based on dictionary words, reinvent them or even end passwords as we know them.

Five years ago, even the author of the strictest rules for passwords conced-

Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!" Algo como: "O homem que escreveu essas regras das passwords tem uma nova recomendação: esqueçam!"

Esse homem é Bill Burr. Ele trabalhava no National Institute of Standards and Technology (NIST) norte-americano quando publicou um pequeno folheto em 2003, "NIST Special Publication 800-63. Appendix A" (entretanto substituído e agrupado nas "Digital Identity Guidelines: Enrollment and Identity Proofing Requirements").

Nele, aconselhava os utilizadores a misturarem símbolos e letras, maiúsculas e minúsculas, para "inventarem novas palavras estranhas", e a mudá-las regularmente para protegerem os seus bens digitais.

O conselho foi seguido por imensas instituições nos EUA e replicado pelo mundo comprador de tecnologia. "O problema é que o conselho acabou por estar em grande parte incorreto, diz Burr. Alterar a password a cada 90 dias? A maioria das pessoas faz pequenas mudanças que são fáceis de adivinhar, lamentou. Alterar Pa55word!1 para Pa55word!2 não mantém os hackers afastados", notou a CloudNine. Até a mistura aleatória de letras, números ou caracteres especiais "não fazem muito para frustrar os hackers".

ed that an irreversible point had been reached, expressed in a Wall Street Journal article titled: 'The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1 d!' Something like, 'The man who wrote those passwords rules has a new recommendation: forget it!'

That man is Bill Burr. He worked at the American National Institute of Standards and Technology (NIST) when he published a small leaflet in 2003, 'NIST Special Publication 800-63. Appendix A' (now replaced and grouped in 'Digital Identity Guidelines: Enrollment and Identity Proofing Requirements').

In it, he advised users to mix symbols and letters, both uppercase and lowercase, to 'invent strange new words', and to change them regularly to protect their digital assets.

The advice was followed by many US institutions and replicated around the technology-buying world. 'The problem is that the advice turned out to be largely incorrect', says Burr. 'Change your password every 90 days? Most people make minor changes that are easy to guess, he lamented. Changing Pa55word!1 to Pa55word!2 doesn't keep the hackers at bay', noted CloudNine. Even the random mix of letters, numbers or special characters 'doesn't do much to foil hackers'.

Burr explicou como não existia muito trabalho prévio ao seu e que se tinha orientado por um "white paper" de segurança dos anos 1980s. A alternativa posterior foi recomendar que se mudasse das palavras-chave (password) para frases-chave (passphrases) fáceis de memorizar e/ou a autenticação de dois fatores (2FA).

Esta autenticação levanta outros problemas, como perceberam recentemente os utilizadores do Twitter quando a empresa foi multada em 150 milhões de dólares pela Federal Trade Commission norte-americana.

A rede social levou os utilizadores a darem o número de telefone para impor um sistema 2FA mas usou-os para fins comerciais, de publicidade, sem autorização e comprometendo a privacidade dos mesmos.

As recomendações mais recentes do NIST sobre a complexidade das passwords já se baseiam em trabalho de análise a milhões de passwords expostas. A instituição salienta que permitem sintetizar como os humanos têm "uma capacidade limitada de memorizar segredos complexos e arbitrários, por isso geralmente escolhem passwords que podem ser facilmente adivinhadas".

Desta forma, "os requisitos de comprimento e complexidade além dos reco-

Burr explained how there was not much work prior to his and that he had been guided by a 1980s white paper on security. The later alternative was to recommend changing from keywords (password) to easy-to-remember key phrases (passphrases) and/or two-factor authentication (2FA).

This authentication raises other problems, as Twitter users recently realised when the company was fined US$150 million by the American Federal Trade Commission.

The social network prompted users to provide their phone number to impose a 2FA system but used them for commercial purposes, advertising, without authorization and compromising their user's privacy.

The latest NIST recommendations on the complexity of passwords are already based on analysis work on millions of passwords exposed. The institution points out that they allow synthesizing how humans have 'only a limited ability to memorise complex, arbitrary secrets, so they often choose passwords that can be easily guessed.'

Thus, 'length and complexity requirements beyond those recommended here significantly increase the difficulty of memorized secrets and increase user

mendados aumentam significativamente a dificuldade dos segredos memorizados e aumentam a frustração do utilizador. Em resultado disso, os utilizadores geralmente contornam essas restrições de maneira contraproducente", além de se saber que "muitos ataques associados ao uso de passwords não são afetados pela [sua] complexidade e tamanho".

O corpo como identificação

Confrontados com este cenário, investigadores da cibersegurança têm procurado alternativas, tanto recorrendo a tecnologias já existentes como a outras emergentes.

O email, por exemplo, é uma identificação que se usa para muito em ambiente

frustration. As a result, users often work around these restrictions in a way that is counterproductive', in addition to knowing that 'many attacks associated with the use of passwords are not affected by password complexity and length.'

The body as identification

Faced with this scenario, cybersecurity researchers have sought alternatives, both using existing and emerging technologies.

Email, for example, is an identification that is used for a lot in an online environment but is a terrible security solution. It is an unfit communication tool to be used as a secure identifier. Who has never received an email addressed to another person in their mailbox? Normally,

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Fonte: Hive Systems

online mas é uma péssima solução de segurança. É uma ferramenta de comunicação, incompetente para ser usada como identificador seguro. Quem nunca recebeu um email endereçado a outra pessoa na sua "mailbox"? Normalmente, são poucos tendo em conta que circulam 319 mil milhões de emails de 4.100 milhões de utilizadores por dia. Ainda assim, é usado como segundo fator em aplicações sem grandes requisitos de segurança, para validar perfis ou recuperar passwords.

Um dos identificadores há muito apontado como sendo o mais seguro e que acompanha sempre os utilizadores é o corpo. Pela identificação digital ou palmar, pela análise da íris ou outras, as tecnologias biométricas estão a ser adaptadas discretamente e de forma funcional em ambientes onde podem falhar sem grandes problemas. Se um leitor da impressão digital à entrada do ginásio falhar, o impacto é mínimo.

O reconhecimento facial é outra tecnologia promissora. Está disponível nos telemóveis, sem levantar qualquer objeção em termos de privacidade sobre quem armazena os dados que permitem validar a verificação de segurança. É uma tecnologia já disponível nos aeroportos e pelas autoridades policiais, usada nalgumas instituições públicas e privadas, com vários erros e enviesamentos raciais e de

there are few, considering that there are 319 billion emails from 4.1 billion users per day. Still, it is used as a second factor in applications with no major security requirements, to validate profiles or retrieve passwords.

One of the identifiers long identified as being the safest and that always accompanies users is the body. By digital or handprint identification, iris or other analysis, biometric technologies are being discreetly and functionally adapted in environments where they can fail without major problems. If a fingerprint reader at the entrance of the gym fails, the impact is minimal.

Facial recognition is another promising technology. It is available on mobile phones, without raising any privacy objection around who stores the data that validate the security check. It is a technology already available at airports and by police authorities, used in some public and private institutions, with various racial and gender errors and biases reported.

The 'use of facial verification increasingly normalises the expectation that our bodies should be used as a form of government ID', when reliable alternative solutions such as the Portuguese Citizen Card exist.

The same can be said of CAPTCHAs, the graphical solution to ensure that there

género reportados.

O "uso da verificação facial normaliza cada vez mais a expectativa de que os nossos corpos devem ser usados como uma forma de identificação do governo", quando existem soluções alternativa fiáveis como o Cartão de Cidadão.

O mesmo pode ser dito dos CAPTCHAs, a solução gráfica para garantir que existe uma identificação de padrões por um humano. Eles podem ser usados como password, a partir da escolha e deteção de alguns elementos gráficos, numa sequência escolhida pelo utilizador.

No ano passado foram gastos "cerca de

is a pattern identification done by a human. They can be used as a password, from the choice and detection of some graphic elements, in a sequence chosen by the user.

Last year alone people spent 'about 500 years a day on CAPTCHAs. It's time to end this madness', which aims only to prove that someone is human. The result obtained accounts that 'it takes a user on average 32 seconds to complete a CAPTCHA challenge. There are 4.6 billion global Internet users. We assume a typical Internet user sees approximately one CAPTCHA every 10 days.'

Since they first appeared in 1997, un-

500 anos por dia em CAPTCHAs. Está na altura de parar com esta loucura" que visa apenas provar que alguém é humano. O resultado foi obtido a partir de "um utilizador gastar em média 32 segundos para completar um desafio de CAPTCHA. Há 4.600 milhões de utilizadores da Internet. Assumimos que um utilizador típico da Internet vê aproximadamente um CAPTCHA a cada 10 dias".

Desde que apareceu o primeiro, em 1997, até se tornar sigla de "Completely Automated Public Turing test to tell Computers and Humans Apart" em 2003, os CAPTCHAs foram criticados e até a analista Gartner notou como são "uma defesa imperfeita contra bots", acabando por recomendar o uso de versões mais "evoluídas".

Os CAPTCHAs começaram por ser usados contra o spam no motor de busca AltaVista. Em seguida, serviram para resolver problemas de IA. "A primeira palavra era conhecida pelo sistema, a segunda palavra não era identificada e fazia parte de uma digitalização de livro. Uma vez que várias pessoas tivessem digitado a mesma resposta para a segunda palavra, ela seria resolvida" para constar na obra.

A Google adquiriu o reCAPTCHA e lançou uma nova versão, que passou a incluir a escolha de imagens. Desta vez, o

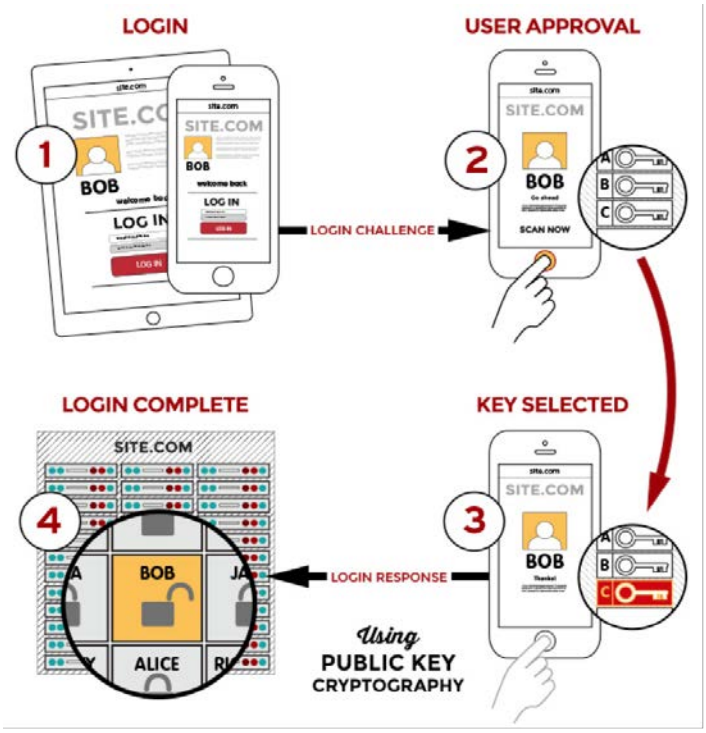
til they became the acronym for 'Completely Automated Public Turing test to Tell Computers and Humans Apart' in 2003, CAPTCHAs have been criticised and even analyst Gartner noted how they are 'an imperfect defence against bots', eventually recommending the use of more 'evolved' versions.

CAPTCHAs were first used against spam by the AltaVista search engine. Then, they were used to solve AI problems. 'The first word was known to the system, the second word was unidentified to the system and was part of a book scan. Once a number of people had typed in the same answer for the second word, it would be resolved' for the book scan.

Google acquired reCAPTCHA and released a new version, which now includes the choice of images. This time, the goal was to solve machine vision problems, useful for autonomous vehicles, accompanying tools of user behaviour analysis. As with QR codes, it was never considered to be a reliable security technology.

It's the user's responsibility

Until we live in a zero-password future, one thing is certain: much of the computer insecurity is due to the users themselves, where '64 percent of consumers repeat passwords for more than one account and 70 percent of passwords that



objetivo era resolver problemas de visão por máquina, útil para os veículos autónomos, acompanhando ferramentas de análise de comportamento do utilizador. Como sucedeu com os códigos QR, nunca se considerou ser uma tecnologia de segurança fiável.

A responsabilidade é do utilizador

Até chegar o futuro sem passwords, há uma constatação: muita da insegurança informática deve-se aos próprios utilizadores, quando "64% repete passwords para mais de uma conta e 70% das pass-

have been compromised are still in use.'

The finding justifies a more technological development to access equipment, much less dependent on the human factor.

Technology companies looking for alternatives talk about this 'passwordless future', as Microsoft announced last year, given that 'passwords are a nuisance to use and present security risks to users and organizations of all sizes, with an average of 1 in every 250 corporate accounts being compromised each month. For Gartner, 20 to 50 % of all technical support calls are for password reset. The World Economic Forum estimates that cybercrime has cost the global economy $2.9 million every minute in 2020 and some 80 % of these attacks are password-related.'

In fact, the company was already supporting the FIDO (Fast IDentity Online) open standard, along with other large companies that need secure authentication protocols to grant their users access. Aggregating large organizations with a common goal facilitates the widespread adoption of the technical solution.

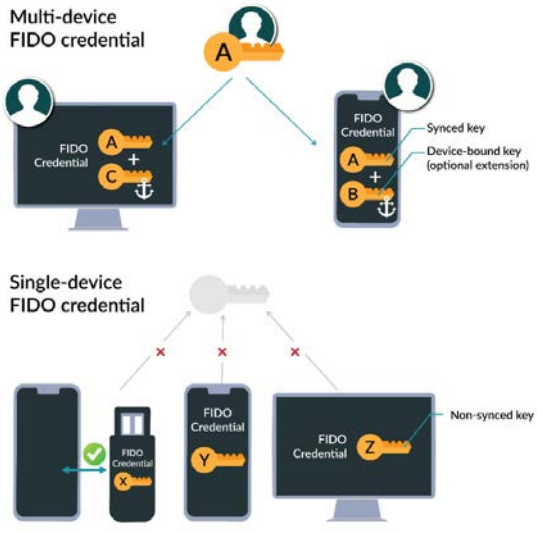
In early May, companies had already

words que foram comprometidas continuam em uso".

A constatação justifica um desenvolvimento mais tecnológico para acesso aos equipamentos, muito menos dependente do fator humano.

Empresas de tecnologia à procura de alternativas falam nesse "futuro sem passwords", como anunciou a Microsoft no ano passado, dado que "as passwords são um incómodo de usar e apresentam riscos de segurança para utilizadores e organizações de todos os tamanhos, com uma média de uma em cada 250 contas corporativas comprometidas a cada mês. Para a Gartner, 20 a 50% de todas as chamadas de suporte técnico são para redefinições de password. O World Economic Forum estima que o cibercrime custou à economia global 2,9 milhões de dólares a cada minuto em 2020, e cerca de 80% desses ataques foram relacionados com passwords".

Na realidade, a empresa já estava a apoiar a norma aberta FIDO (Fast IDentity Online), junto com outras grandes empresas que precisam de protocolos de autenticação segura para darem acesso aos seus utilizadores. A agregação de grandes organizações com um objetivo comum facilita a adoção generalizada da solução técnica.



pre-announced their intentions. Apple, Google and Microsoft confirmed more vigorous support for the initiative, including more than a hundred organisations such as Amazon, American Express, Bank of America, Intel, Qualcomm, Meta or Yahoo! Japan, which announced that more than half of its 50 million users were already using it.

The FIDO Alliance was formed in 2012 and, two years later, the first version was published, with the two protocols FIDO U2F (Universal Second Factor) and FIDO UAF (Universal Authentication Framework). Both are part of version 2, which also incorporated the W3C Webauthn (World Wide Web Consortium's Web Authentication Standard), the CTAP1 (ex-FIDO U2F) and CTAP2 Client-to-Au-

No início de maio, empresas que já tinham pré-anunciado as suas intenções - Apple, Google e Microsoft - confirmaram um apoio mais vigoroso à iniciativa, onde figuram mais de uma centena de organizações como a Amazon, American Express, Bank of America, Intel, Qualcomm, Meta ou a Yahoo! Japão, que anunciou já ter mais de metade dos seus 50 milhões de utilizadores a usarem-na.

A FIDO Alliance surgiu em 2012 e, dois anos depois, foi publicada a primeira versão, com os dois protocolos FIDO U2F (Universal Second Factor) e FIDO UAF (Universal Authentication Framework). Ambos estão na versão 2, que passou a incorporar o W3C WebAuthn (Web Authentication Standard do World Wide Web Consortium), os Client-to-Authenticator Protocols CTAP1 (ex-FIDO U2F) e CTAP2 e o FIDO UAF.

De forma mais simples, a norma já é suportada nos sistemas operativos Windows, iOS e Android e nos browsers Chrome, Edge e Firefox. Ela assegura uma "experiência de utilizador sem password, segundo-fator [2FA] e multi-fator [MFA] com autenticadores incorporados (ou vinculados) - como biométricos ou PINs - ou autenticadores externos (ou roaming) - como FIDO Security Keys, dispositivos móveis, 'wearables', etc.)", refere a organização.

thenticator Protocols and the UAF FIDO.

To put it in simply, the standard is already supported by Windows, iOS and Android operating systems and on Chrome, Edge and Firefox browsers. It supports a 'passwordless, second-factor [2FA] and multi-factor [MFA] user experiences with embedded (or bound) authenticators (such as biometrics or PINs) or external (or roaming) authenticators (such as FIDO Security Keys, mobile devices, wearables, etc.)' states the organization.

The system is not based on passwords but rather on an evolution to encrypted passkeys. In practice, FIDO replaces passwords with encrypted data stored on the local device that can be used on different equipment or applications.

The passkeys require a FIDO credential manager - a second-factor or 'authenticator' of digital, facial or PIN recognition, for example - to validate identity in online access.

Personal information is created and encrypted as a private key on that authenticator device (for example, a mobile phone), while a public key is sent to an account on the online service you want to access. This also facilitates secure online access to equipment not normally used by the user.

O sistema não se baseia em passwords mas numa evolução para "passkeys" cifradas. Na prática, a FIDO substitui as passwords por dados cifrados, armazenados no dispositivo local e que podem ser usados em diferentes equipamentos ou aplicações.

As "passkeys" obrigam a ter um gestor de credenciais FIDO - um segundo-fator ou "autenticador" de reconhecimento digital, facial ou de PIN, por exemplo - para validar a identidade no acesso online.

A informação pessoal é criada e cifrada como uma "private key" nesse dispositivo "autenticador" (um telemóvel, por exemplo), enquanto uma "public key" é enviada para uma conta no serviço online a que se pretende aceder. Isto também facilita o acesso seguro online em equipamentos normalmente não usados pelo utilizador.

É esta alegada facilidade de utilização, com soluções alternativas, que pode dinamizar e generalizar o uso da norma. Uma password pode ser esquecida, confundida, fácil de descobrir, ao contrário do reconhecimento biométrico. Agora, diz a Alliance, "os utilizadores farão login por meio da mesma ação que realizam várias vezes ao dia para desbloquear os seus dispositivos, como uma simples verificação de impressão digital ou facial ou um PIN do dispositivo. Essa nova

It is this alleged ease of use, with alternative solutions, which can streamline and generalise the use of the standard. A password can be forgotten, confused, easy to find out, unlike biometric recognition. Now, Alliance says, 'users will sign in through the same action that they take multiple times each day to unlock their devices, such as a simple verification of their fingerprint or face, or a device PIN. This new approach protects against phishing and sign-in will be radically more secure when compared to passwords and legacy multi-factor technologies such as one-time passcodes sent over SMS.'

This will make it possible to 'log in without having to type a password, which is faster and much more convenient. Equally important, the credential can be stored online so that it's available when I replace or lose my current phone, solving another problem that has plagued some MFA users — the risk of being locked out of accounts when phones are lost or stolen.

The recovery processes works by using an already authenticated device to download the credential, with no password required. This is really the issue here - there is no recovery process, as the private key is immediately available on a user's devices,' explains Andrew Shikiar, FIDO Alliance's CEO.

abordagem protege contra phishing e o login será radicalmente mais seguro quando comparado a passwords e a tecnologias multifatoriais herdadas, como senhas de uso único enviadas por SMS".

Será assim possível "fazer login sem precisar de digitar uma password, o que é mais rápido e muito mais conveniente. Igualmente importante, a credencial pode ser armazenada online para que esteja disponível quando se substituir ou perder o telefone atual, resolvendo outro problema que tem atormentado alguns utilizadores de MFA – o risco de terem as suas contas bloqueadas quando os telefones são perdidos ou roubados.

Os processos de recuperação funcionam usando um dispositivo já autenticado para transferir a credencial, sem necessidade de password. 'Essa é realmente a questão aqui – não há processo de recuperação, pois a chave privada está imediatamente disponível nos dispositivos de um utilizador', explica Andrew Shikiar, diretor executivo da FIDO Alliance".

Recomendações para a criação e gestão de passwords

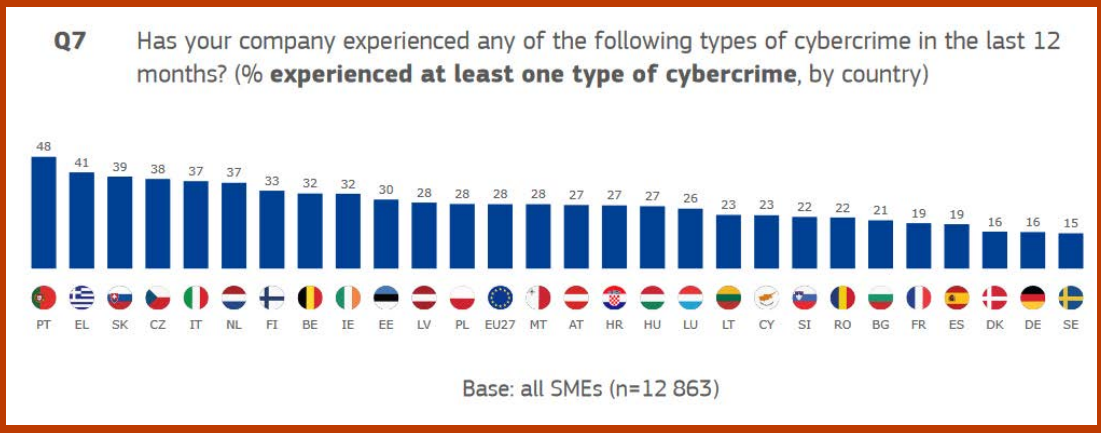
- O mais longa possível.
- Utilização de caracteres variados.
- Não incluir informações pessoais.
- Múltiplos-fatores de autenticação.
- Usar Software de Gestão de Passwords.

Fonte: As chaves da nossa casa digital

Recommendations for creating and managing passwords

- Make them as long as possible.
- Use a variety of characters.
- Do not include personal information.
- Use multi-factor authentication.
- Use Password Management Software.

Source: The keys to our digital home



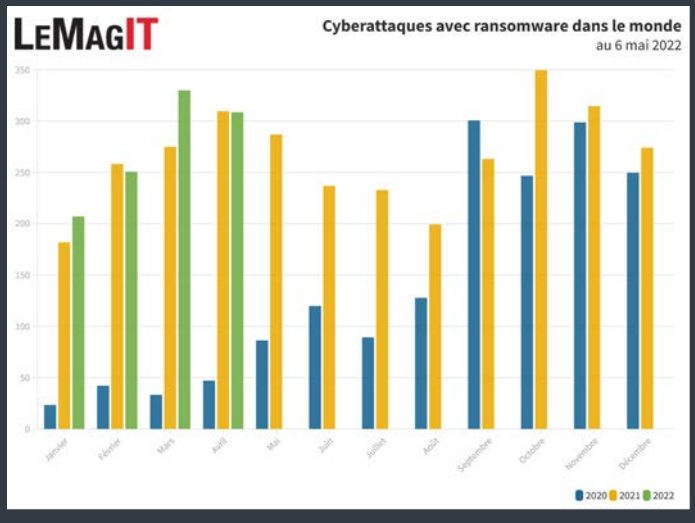
Como o cibercrime atinge as PMEs portuguesas

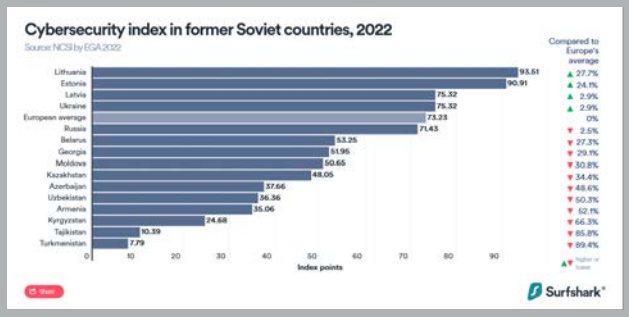
Quase metade (48%) das PMEs portuguesas sofreu um ciberataque de qualquer tipo nos últimos 12 meses, quando a média europeia é de 28%. Na Suécia, essa percentagem chegou apenas aos 15%. Este e outros dados constam do relatório europeu "SMEs and cybercrime".

How cybercrime affects Portuguese SMEs

Almost half (48 %) of Portuguese SMEs have suffered a cyberattack of any kind in the last 12 months, when the European average is 28 %. In Sweden, this percentage reached only 15 %. This and other data are included in the European report 'SMEs and cybercrime'.

Ciberataques com ransomware em todo mundo (até Maio) Worldwide cyberattacks with ransomware (until May)





Cibersegurança nos ex-países soviéticos

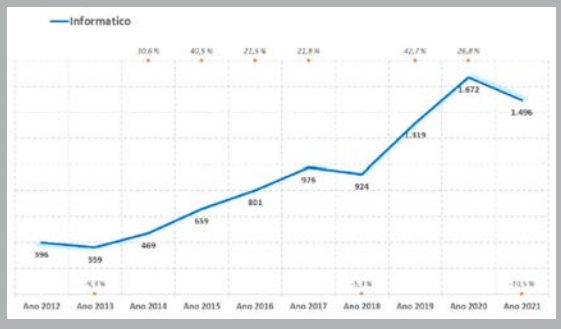
Lituânia, Estónia, Letónia e Ucrânia lideram, por esta ordem, os níveis de cibersegurança nos antigos países da União Soviética à frente da média da União Europeia. A Rússia está ligeiramente abaixo dessa média.

Cibersecurity in former Soviet countries

Lithuania, Estonia, Latvia and Ukraine lead cybersecurity levels in former Soviet countries, in this order, ahead of the European Union average. Russia is slightly below that average.

Para onde vai o crime informático?

Em 2021, os crimes informáticos diminuíram em pequena escala (-10,5%), refere o Relatório Anual de Segurança Interna. A previsão é que tenda a aumentar na "criminalidade associada a tecnologias apoiadas em blockchain, acessos ilegítimos a carteiras de criptomoedas, aumento de ofuscação de intenções criminosas através de formas de programas maliciosos ligados a extorsão (ransomware) com o verdadeiro objetivo de sabotagem".



Where is computer crime heading to?

In 2021, computer crime decreased on a small scale (-10.5 %), says the Annual Internal Security Report. The forecast is that it tends to increase in 'criminality associated with blockchain-supported technologies, illegitimate access to cryptocurrency portfolios, increased obfuscation of criminal intent through forms of malicious programs linked to extortion (ransomware) with the real purpose of sabotage.'

3

Cristina Almeida

Presidente da Women4Cyber Portugal
President at Women4Cyber Portugal

1. O que é a Women4Cyber (W4C PT), quais os objetivos e projetos para 2022?

A W4C PT é o capítulo português da Fundação Women4Cyber, sediada na Bélgica, e tem como missão promover e apoiar a participação das mulheres na área da cibersegurança.

Até ao final do ano, a nível global, a organização vai lançar duas plataformas: Women4Cyber Academy, que irá possibilitar que jovens de todo o mundo consigam adquirir conhecimentos de cibersegurança gratuitamente; e a Job Platform que tem como intuito partilhar oportunidades de emprego. Paralelamente, existem também os programas de mentoria internacionais.

Em Portugal, a nossa estratégia passa por trabalhar em rede e potenciar parcerias que nos permitam cumprir a nossa missão. Vamos continuar a desenvolver o nosso programa de "Role Models" - dando visibilidade às mulheres que trabalham atualmente na

1. What is Women4Cyber (W4C PT) and what are its goals and projects for 2022?

W4C PT is the Portuguese chapter of the Women4Cyber Foundation, headquartered in Belgium, and its mission is to promote and support the participation of women in the area of cybersecurity.

Until the end of the year, the organization will launch two platforms on a global scale: Women4Cyber Academy, which will enable young people from around the world to acquire knowledge on cybersecurity for free; and the Job Platform, which aims to share job opportunities. At the same time, there are also international mentoring programmes.

In Portugal, our strategy involves working online and leveraging partnerships that allow us to fulfil our mission. We will continue to develop our Role Models program - giving visibility to women who currently work in the area - and focus on content creation, with an accessible language and with the aim of responding to the contacts and support requests we have received, namely to make a career transition.

In addition, we are planning on launching a podcast focused on fighting misinformation, among other things. Each season will feature several experts and will address a different theme. The first season will focus on the diversity of areas where it is possible to build a professional career, from the legal

área - e focar-nos na criação de conteúdos, com uma linguagem acessível e com o objetivo de responder aos contatos e pedidos de apoio que temos recebido, nomeadamente, para fazer a transição de carreira.

Adicionalmente, temos previsto o lançamento de um podcast focado, entre outros assuntos, no combate à desinformação. Cada temporada contará com diversos especialistas e abordará uma temática diferente. A primeira temporada será focada na diversidade de áreas onde é possível fazer uma carreira profissional, desde a vertente legal à investigação, por exemplo. Desta forma esperamos informar e criar um espaço de diálogo que encoraje mais jovens profissionais a fazer a transição.

2. No Estudo sobre o Ensino Pós-Secundário e o Ensino Superior de Cibersegurança em Portugal, do CNCS, há vários cursos com conteúdos sobre cibersegurança, mas a percentagem de inscritas é muito baixa. A que se deve esta baixa procura e aparente desinteresse?

Foi com tristeza que verificámos que as inscrições de raparigas continuam substancialmente aquém e que representam um aumento de apenas 1% face ao ano anterior. Estes resultados sugerem-nos que as jovens não consideram uma carreira nesta área e nós acreditamos que a falta de informação é uma das grandes causas. Desde que a pandemia começou, nunca se falou tanto de

side of it to research, for example. In this way we hope to inform and create a space for dialogue that encourages more young professionals to make the transition.

2. In CNCS' Study on Post-secondary Education and Higher Education in Cybersecurity in Portugal, there are several courses with curricula on cybersecurity, but the percentage of students enrolled in them is very low. What is the reason for these low enrolment numbers and apparent disinterest?

It is with sadness that we have seen that girls' enrolments are still substantially lower and represent an increase of only 1 % compared to the previous year. To us, these results suggest that young women do not consider a career in this area, and we consider one of the major causes to be the lack of information. Since the pandemic began, there has never been so much talk of cybersecurity, but there is still a very limited idea of the possibilities within the area.

For example, the entertainment industry feeds the idea that cybersecurity is only for underground hackers; however, in the real world, opportunities are very diverse. We need to work out existing prejudices and stereotypes, since we cannot exclude 50 % of the population from a structuring area of our society.

cibersegurança, mas a verdade é que continua a haver uma ideia muito limitada das possibilidades dentro da área. Por exemplo, a indústria do entretenimento alimenta a ideia de que cibersegurança é só para "hackers" na clandestinidade; no entanto, no mundo real, as oportunidades são muito diversas. Temos de trabalhar preconceitos e estereótipos existentes, uma vez que não podemos excluir 50% da população de uma área estruturante da nossa sociedade.

3. Mas como inverter a situação e "começar uma carreira em cibersegurança"?

Hoje enfrentamos uma grande carência de profissionais em cibersegurança a nível europeu que precisa de ser endereçada o mais rapidamente possível. E, neste caso, o redireccionamento de carreira é fundamental, apoiando ativamente as mulheres que querem ingressar na área, através de formação formal, assim como de criação de mentorias e outras redes de apoio.

Paralelamente, e apesar de a ausência de mulheres em posições de liderança ser um espelho da sociedade em que vivemos, é importante destacar que existem atualmente mulheres em lugares de destaque, em Portugal. E, neste campo, lamentamos não ter visto um painel de debate ou espaço de comentário/análise de ciberataques que tenha tido uma representação feminina. Perdeu-se uma boa oportunidade de trazer diversidade para a esfera pública.

3. But how can one reverse the situation and 'start a career in cybersecurity'?

Today, we face a great shortage of cybersecurity professionals at a European level, one that needs to be addressed as soon as possible. And, in this case, career redirection is essential, actively supporting women who want to enter the area, through formal training, as well as the creation of mentoring and other support networks.

At the same time, and although the absence of women in leadership positions is a mirror of the society we live in, it is important to highlight that, in Portugal, there are currently women in prominent seat. In this field, we regret not having seen a debate panel or a comment/analysis space on cyberattacks with a female representation. A good opportunity to bring diversity into the public sphere has been missed.

José Ramos

Analista de cibersegurança do .PT

.PT Cybersecurity Analyst

Autenticação de dois fatores (2FA)

Verificamos o contínuo crescimento, quer em número, quer em sofisticação, do cibercrime e do impacto causado no normal funcionamento das atividades socioeconómicas. O foco continua a ser a exfiltração de dados pessoais/sensíveis através da obtenção de credenciais para infiltração nas redes das organizações. Segundo o relatório "The Global Risks Report 2022" publicado pelo World Economic Forum, a apresentação dos cyber-riscos emergentes ao mais alto nível da hierarquia de uma organização, irá fortalecer a resiliência e consciencialização para a cibersegurança.

No contexto português, particularmente no início de 2022, algumas entidades foram alvo de ciberataques, nomeadamente órgãos de comunicação social, operadoras de telecomunicações e outras empresas relevantes devido à sua exposição mediática. Em particular, sobre um dos ciberataques ocorridos no início do ano, especulou-se que um dos vetores de ataque foi ultrapassar o duplo fator de autenticação (2FA) com recurso à clonagem do cartão de telemóvel ("SIM swapping") de um colaborador, o que demonstra a sofisticação e os recursos utilizados pelos cibercriminosos.

Two-factor authentication (2FA)

We see the continued growth of cybercrime, both in numbers and in sophistication, and its impact on the normal functioning of socio-economic activities. The focus continues to be the exfiltration of personal/sensitive data by obtaining credentials for infiltration in organizations' networks. According to 'The Global Risks Report 2022' by the World Economic Forum, the presentation of emerging cyber risks at the highest level of an organization's hierarchy will strengthen resilience and awareness for cybersecurity.

In the Portuguese context, particularly in early 2022, some entities were the target of cyberattacks, including media companies, telecommunications operators and other relevant companies due to their mediatic exposure. Regarding one cyberattack in particular that took place earlier in the year, it was speculated that one of the attack vectors was to overtake the two-factor authentication (2FA) by SIM swapping a collaborator's mobile phone card, which shows the sophistication and resources used by cybercriminals.

Em que consiste o duplo fator de autenticação?

Interessa perceber nesta análise o que é o duplo fator de autenticação, sendo este um mecanismo que adiciona um nível extra de segurança ao solicitar que o utilizador se autentique através de dois métodos diferentes. Por definição, considera-se que o duplo fator de autenticação utiliza dois dos três métodos seguintes para confirmar uma identidade:

• algo que sabemos: password, perguntas de segurança, PINs;

• algo que temos: coisas na posse dos utilizadores, por exemplo, smartphones, tokens de hardware;

• algo que somos: provar que o utilizador é a pessoa que afirma ser, geralmente fatores biométricos (impressão digital ou identificação facial).

Vantagens do duplo fator de autenticação?

Como referido, o duplo fator de autenticação pode ser comprometido. É preciso ter consciência de que nenhum sistema é seguro e por mais mecanismos de segurança que sejam implementados, estes podem ser explorados e comprometidos dependendo apenas

What is two-factor authentication?

It is important to understand that two-factor authentication is a mechanism that adds an extra level of security by requesting the user to go through two different authentication methods. By definition, the two-factor authentication is considered to use two of the following three methods to confirm an identity:

• something we know: password, security questions, PINs;

• something we have: something in the user's possession, like a smartphones, hardware tokens;

• something we are: to prove the user is the person they claim to be, usually biometric factors (fingerprinting or facial identification).

Advantages of two-factor authentication?

As stated, the two-factor authentication can be compromised. We must be aware that no system is safe and no matter how many security mechanisms are implemented, they can be exploited and compromised depending only on their complexity and the imagination/ resources of malicious agents.

da sua complexidade e da imaginação/ recursos dos agentes maliciosos.

Mesmo assim, importa referir as vantagens em implementar um mecanismo de duplo fator de autenticação, sendo que a primeira será sempre a segurança:

• fácil de usar e implementar;

• prevenção de fraude e roubo de identidade;

• aumento da confiança no sistema por parte do utilizador;

• conformidade com várias normas internacionais;

• reduz o risco das passwords: a boa prática é utilizar passwords complexas e exclusivas, a melhor prática é a utilização de um duplo fator de autenticação.

Ativar o duplo fator de autenticação no Sistema de Registo .PT

Tendo consciência de que o Duplo Fator de Autenticação não vai resolver todos os problemas de segurança, importa salientar a importância desta camada de segurança, que deve ser ativada sempre que tal for possível. Assim, apresentamos os passos para ativar este mecanismo no Sistema de Registo e Gestão de Domínios .PT:

Even so, it is important to mention the advantages of implementing a two-factor authentication mechanism, the first being always security:

• easy to use and implement;

• prevention of fraud and identity theft;

• increases user confidence in the system;

• compliance with various international standards;

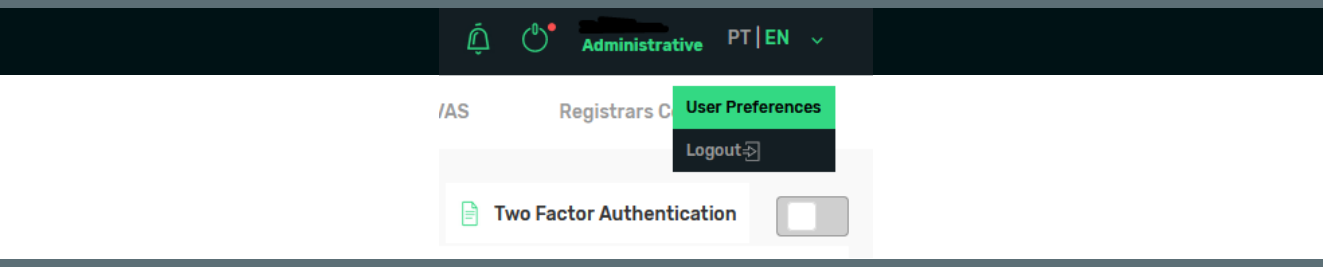
• reduces the risk of passwords: good practice is to use complex and exclusive passwords, best practice is to use a two-factor authentication.

Enable two-factor authentication in the .PT Domain Registration

Being aware that the Two-Factor Authentication will not solve all security problems, it is important to stress the importance of this security layer, which should be activated whenever possible. Thus, we present the steps to activate this mechanism in the .PT Domain Registration and Management System:

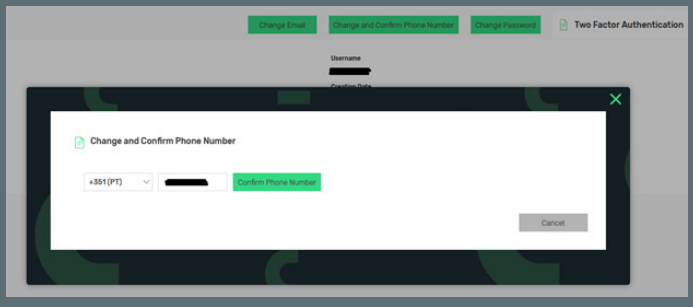
1 – Após o login, o utilizador deve clicar no seu nome e de seguida clicar em "User Preferences".

1 - After logging in, the user must click on their name and then on 'User Preferences'.



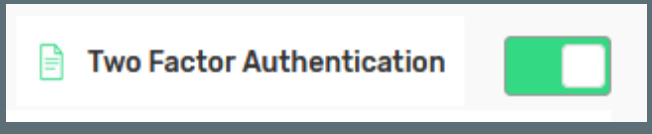
2 – O utilizador deve definir o seu número de telemóvel na janela que aparece após clicar em "Change and Confirm Phone Number". Após preencher o campo destinado ao número de telemóvel, deve clicar em "Confirm Phone Number".

2 - Enter their mobile phone number in the window that appears after clicking on 'Change and Confirm Phone Number'. After entering the mobile phone number, it is recommended to click on 'Confirm Phone Number'.



3 – Para finalizar, o utilizador deve então ativar o Duplo Fator de Autenticação.

3 - To finish, activate the Two-Factor Authentication.



DBIR 2022

O 2022 Data Breach Investigations Report (DBIR) da operadora norte-americana Verizon confirma que o ransomware continuou a aumentar no ano passado, seguindo a tendência dos últimos cinco anos. Mas o ransomware "é apenas um modelo de monetizar o acesso a uma organização", já antes fragilizada pela obtenção ilegal de credenciais, phishing, exploração de vulnerabilidades e botnets. 82% destes casos têm intervenção do "elemento humano"

The 2022 Data Breach Investigations Report (DBIR) by the American operator Verizon confirms that ransomware continued to increase in 2021, following the trend of the last five years. But ransomware 'is really just a model of monetizing an organization's access', already weakened by the illegal obtaining of credentials, phishing, vulnerabilities and botnets. 82 % of these cases have 'human element' intervention.

Referencial para competências

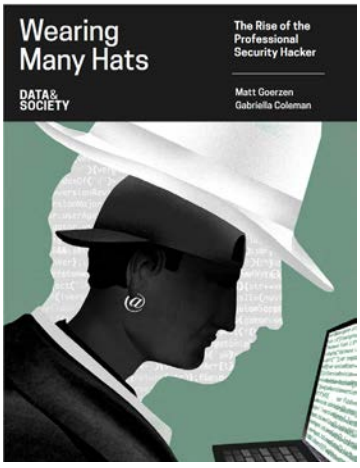
O Centro Nacional de Cibersegurança (CNCS) disponibilizou um Referencial de Competências em Cibersegurança para interessados na formação e contratação de profissionais com capacidades na área. O documento "pretende servir de suporte ao desenvolvimento do setor", contribuindo "para a definição e formulação de políticas públicas neste domínio".

Skills Framework

The Portuguese National Cybersecurity Center (CNCS) created a Cybersecurity Skills Framework for those interested in training and hiring professionals with skills in this area. The document 'aims to support the development of the sector', contributing 'to the definition and creation of public policies in this area.'

Wearing Many Hats: The Rise of the Professional Security Hacker

Dos anos 1980 até este século, esta é uma história sobre a legitimação dos hackers, evoluindo de subcultura até ser um emprego respeitado, com cobertura mediática favorável e "status" cultural - presentes no hacktivismo ao serviço dos direitos humanos ou em áreas da sociedade civil carentes de iniciativas mais institucionais.



From the 1980s to this century, this is a story about the legitimization of hackers, evolving from subculture to a respected job, with favourable media coverage and cultural status - present in hacktivism at the service of human rights or in areas of civil society lacking more institutional initiatives.

#IPv4flagday

1 de Fevereiro de 2030 é dia de remover o IPv4. Empresas de software e de conteúdos, bem como ISPs, vão acabar com a retrocompatibilidade e favorecer o IPv6. Esta alteração afeta apenas os sites que não estão preparados para suportar o IPv6. O seu está?

The 1st of February 2030 is the day to remove IPv4. Software and content companies, as well as IPSs, will end backward compatibility and favour IPv6. This change affects only websites that are not prepared to support IPv6. Is yours?

Estratégia de cibersegurança em Itália

A agência de cibersegurança italiana (ACN) divulgou dois documentos sobre a estratégia nacional de cibersegurança e a sua implementação entre 2022 e 2026.

Cybersecurity strategy in Italy

The Italian Cyber Security Agency (ACN) released two papers on the national cybersecurity strategy and its implementation between 2022 and 2026.

Directora | Director
Inês Esteves

Edição | Editor
Pedro Fonseca

Design Gráfico | Graphic Design
Sara Dias

Tradução | Translation
Sara Pereira

Fotografia (capa e índice) | Photography (cover & index)
Jason Leung on Unsplash
Amol Tyagi on Unsplash

Publicação trimestral | Quarterly publication
Julho 2022 | July 2022

Co-financed by the Connecting Europe Facility of the European Union