BACK 2 BASICS

# SEGURANÇA

## UM MANUAL DE CIBERSEGURANÇA

universidade de aveiro

Co-funded by
the European Union

**Disclaimer: 2021-1-PT01-KA220-HED-000023543**
Este projeto foi financiado com o apoio da Comissão Europeia. Esta publicação e todo o seu conteúdo refletem apenas as opiniões do autor, não podendo a Comissão ser responsabilizada por qualquer utilização que possa ser feita da informação nela contida.

# BACK 2 BASICS

## UM MANUAL DE CIBERSEGURANÇA



Um guia completo das melhores práticas de cibersegurança que permite aos indivíduos e às organizações protegerem-se contra as ameaças comuns no mundo digital.

universidade de aveiro

BIO LIVING

HELLENIC REPUBLIC UNIVERSITY OF MACEDONIA

gri

**Título**
SEGURANÇA - Um manual de cibersegurança

**Projeto**
Back2Basics - Colmatar o fosso entre o ensino superior e o mercado de trabalho através da promoção de competências digitais

**Referência do projeto**
Erasmus+ 2021-1-PT01-KA220-HED-000023543

**Coordenação**
João Rafael Almeida [Gabinete de Cibersegurança da Universidade de Aveiro]
Cristina Cerqueira [Gabinete de Cibersegurança da Universidade de Aveiro] João Paulo Barraca [Gabinete de Cibersegurança da Universidade de Aveiro]
Rita Santos [Departamento de Comunicação e Arte/Digimédia, Universidade de Aveiro]

**Contribuições | Parceiros (por ordem alfabética)**
Associação BioLiving
GRI - Gabinete de Recolha Industrial Universidade de Aveiro
Universidade da Macedónia

**Design gráfico**
Gonçalo Gomes [Departamento de Comunicação e Arte/ID+, Universidade de Aveiro]

**Editora**
UA Editora Universidade de Aveiro

**ISBN**
XXX-XXX-XXX-XXX

**DOI**
XXX-XXX-XXX-XXX

## RESUMO



Num mundo cada vez mais interligado, a cibersegurança é de extrema importância. Este manual serve como um recurso valioso para indivíduos e organizações que procuram navegar no cenário em constante evolução das ciberameaças. Abrangendo tópicos que vão desde a engenharia social e o phishing até à prevenção de malware e autenticação multi-fator, este guia abrangente fornece conselhos práticos e melhores práticas para mitigar os riscos. Este manual permite que os leitores protejam os seus ativos digitais e mantenham uma presença online segura, promovendo a sensibilização para a cibersegurança, realçando a importância de medidas pró-ativas e oferecendo orientações para a manutenção de defesas robustas. Quer se trate de um indivíduo preocupado com a segurança pessoal ou de uma organização que procura melhorar os seus protocolos de cibersegurança, este manual fornece-lhe os conhecimentos e as ferramentas necessárias para navegar no mundo digital com segurança e confiança.

BACK 2 BASICS

# 1 INTRODUÇÃO

UM MANUAL DE CIBERSEGURANÇA

# INTRODUÇÃO



No mundo interconectado de hoje, onde a tecnologia se tornou parte integrante da nossa vida quotidiana, a importância da cibersegurança não pode ser subestimada. Desta forma, esta foi uma das competências essenciais consideradas no projeto "Back2Basics - Aproximar o ensino superior e o mercado de trabalho promovendo competências digitais", Erasmus+ (2021-1-PT01-KA220-HED- 000023543), que visa abordar a transformação digital no sistema de ensino superior e aproximar os sistemas de ensino superior e os mercados de trabalho, trabalhando na melhoria das competências digitais.

Este manual abrangente foi concebido para dar aos indivíduos os conhecimentos fundamentais necessários para navegar no cenário em constante evolução das ciberameaças, protegendo-os contra potenciais riscos. Embora a era digital tenha trazido enormes benefícios, também expôs a nossa informação a uma vasta gama de potenciais problemas que podem resultar em graves consequências. Ao compreender estas questões, as




pessoas podem reconhecer melhor a importância da cibersegurança na sua vida pessoal e profissional.

O aumento insidioso dos ataques de engenharia social realça a sofisticação crescente dos cibercriminosos, que empregam táticas psicológicas para manipular indivíduos insuspeitos para que divulguem informações sensíveis ou se envolvam em ações que comprometam a sua segurança - os e-mails de phishing são um excelente exemplo desta estratégia. O phishing envolve e-mails ou websites fraudulentos concebidos para enganar as pessoas, levando-as a partilhar informações pessoais, como palavras-passe ou detalhes de cartões de crédito. Ser vítima de tais ataques pode levar a perdas financeiras, roubo de identidade e danos à reputação. Além disso, a prevalência de malware representa uma ameaça significativa para indivíduos e organizações. O malware é um software concebido para fins maliciosos. Este tipo de software pode infetar computadores

ou redes e comprometer os dados, segurança e integridade do sistema. Por exemplo, o ransomware é um tipo de malware que encripta ficheiros valiosos na máquina alvo e exige um resgate para a sua libertação. Organizações de todos os tamanhos foram vítimas de tais ataques, resultando em perdas financeiras, interrupções operacionais e danos à sua reputação.

Um dos principais objetivos deste manual é sensibilizar o público em geral para a importância da cibersegurança. O manual abordará vários tópicos, incluindo engenharia social, phishing, prevenção de malware, gestão de palavras-passe, autenticação multifatorial, entre outros. Fornecerá conselhos práticos, melhores práticas e exemplos do mundo real para capacitar os leitores a salvaguardar as suas vidas digitais e a atenuar os riscos associados às ciberameaças. Nos capítulos seguintes, algumas das medidas e estratégias proativas que podem ser usadas para se manter seguro no mundo digital são exploradas. Ao desenvolver uma base sólida em ciber sensibilização para a segurança e adoção de práticas defensivas eficazes, as pessoas podem construir coletivamente um ambiente digital mais seguro e resistente para todos.

BACK 2 BASICS

# 2

UM MANUAL DE CIBERSEGURANÇA

# AMEAÇAS COMUNS

# AMEAÇAS COMUNS

O contexto de uma ameaça em cibersegurança deve ser visto como um potencial precursor de um incidente indesejado que pode resultar em danos para dados, sistemas, indivíduos ou organizações. Esta secção apresenta uma visão geral das ameaças comuns para os indivíduos.

## ENGENHARIA SOCIAL

A engenharia social vai além de uma tática enganosa utilizada pelos cibercriminosos para manipular os indivíduos no sentido de revelarem informações sensíveis ou realizarem ações que possam comprometer a sua segurança. Esta técnica não se limita ao ciberespaço e pode ocorrer fora dele, com o objetivo de recolher informações privilegiadas sobre um sistema específico, que podem ajudar os atacantes a serem bem-sucedidos. Aproveita-se da psicologia humana e explora as nossas ten-

dências inerentes, como a confiança, a curiosidade ou o desejo de ajudar os outros. Porque é que isto é importante? A engenharia social tem por objetivo levar as pessoas a tomar decisões sem pensar muito no que está a acontecer, o que pode ser vantajoso para os atacantes que exploram vulnerabilidades nesses processos. Em última análise, o principal objetivo é obrigar um alvo a tomar uma ação específica sem pensar bem no assunto. Quanto mais as pessoas refletirem sobre as ações que estão a tomar, maior será a probabilidade de reconhecerem que essas ações fazem parte de uma manipulação.

Por exemplo, considere um anúncio de televisão com uma artista famosa. O anúncio começa num cenário sombrio com uma música triste, retratando a artista num ambiente deprimente. A cena muda então para um local diferente, onde se veem cães que parecem angustiados e subnutridos, evocando uma sensação de desespero. A artista explica que, sem os nossos donativos, os animais não sobreviverão. Após estas cenas pungentes, a artista reaparece, agora alegre e rodeada de cães saudáveis acompanhados por uma canção entusiástica. Qual é a mensagem subjacente? O anúncio sugere que, por uma pequena doação, a situação destes pobres animais pode ser transformada e eles podem partilhar o seu amor com o público. Embora a intenção possa não ser egoísta, este anúncio tem como objetivo manipular as emoções do público, suscitando sentimentos positivos quando as pessoas contribuem para salvar os cães.



O mesmo princípio pode ser aplicado para fins maliciosos. Numa situação hipotética em que um atacante pretende aceder a uma empresa específica, esse indivíduo pode manipular a atenção do rececionista para contornar a primeira barreira humana. Exemplos dessas estratégias podem incluir a criação

de um sentido de urgência, como alegar uma necessidade urgente de manutenção numa parte específica do edifício. Embora este exemplo possa parecer trivial, é importante reconhecer que a engenharia social não se limita ao ciberespaço.

Os cibercriminosos concebem meticulosamente os seus ataques para parecerem legítimos, explorando vulnerabilidades humanas comuns para atingir os seus objetivos maliciosos. No ciberespaço, estes ataques podem assumir várias formas, como o phishing, o pretexto, o engodo ou mesmo a manipulação física. O sucesso dos ataques de engenharia social

depende muitas vezes da criação de um sentimento de urgência, da exploração da confiança ou do aproveitamento de fatores emocionais. Por exemplo, um atacante pode criar uma mensagem de correio eletrónico fazendo-se passar por um representante de um banco, alegando que a conta do destinatário foi comprometida e instando-o a clicar numa ligação para resolver o problema. Estas táticas manipulam os indivíduos para que atuem sem avaliar criticamente a situação, contornando o seu ceticismo normal. Para se protegerem contra ataques de engenharia social, as pessoas devem manter-se vigilantes e desenvolver um ceticismo saudável quando se envolvem em qualquer forma de comunicação. É essencial verificar a autenticidade dos pedidos, especialmente se envolverem informações sensíveis ou ações inesperadas. Esta verificação pode ser conseguida contactando de forma independente a organização ou pessoa através de um canal de comunicação de confiança para confirmar a legitimidade do pedido. Ao adotar uma abordagem cautelosa e ao manter-se informado sobre as mais recentes técnicas de engenharia social, os indivíduos podem melhorar a sua capacidade de se protegerem contra estas táticas enganosas.



## PHISHING, VISHING E SMISHING

Uma forma comum de engenharia social é o phishing, em que os atacantes enviam e-mails fraudulentos que parecem vir de organizações ou indivíduos respeitáveis. Estas mensagens contêm frequentemente pedidos urgentes, ofertas sedutoras ou alertas alarmantes, com o objetivo de levar os destinatários a tomar medidas imediatas. Podem pedir informações sensíveis, como palavras-passe, números de cartão de crédito ou

credenciais de início de sessão, sob o pretexto de uma necessidade legítima. Estes ataques manifestam-se de várias formas, incluindo phishing por correio eletrónico, smishing (phishing baseado em SMS) e phishing por voz (vishing). O phishing de correio eletrónico é o tipo mais comum, com atacantes a enviarem mensagens de correio eletrónico que parecem genuínas, utilizando frequentemente logótipos oficiais, linguagem e elementos de design para enganar os destinatários. O smishing e o vishing utilizam táticas semelhantes, mas através de mensagens de texto ou chamadas telefónicas, respetivamente.

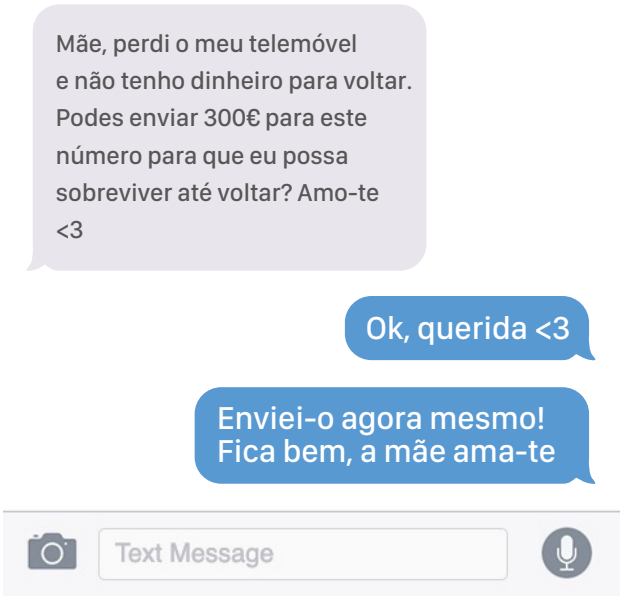
O objetivo de tais ataques pode ser dividido em vários fins:

- **Entrega de cargas maliciosas - a parte de um software malicioso que executa ações maliciosas - que fornecem acesso remoto aos atacantes;**
- **Roubar as credenciais da vítima;**
- **Recolha de outras informações que possam ser utilizadas para escalar outro ataque.**

Para além destas mensagens genéricas que atingem um público alargado, existe uma técnica mais personalizada conhecida como spear phishing. Este método requer alguma preparação do ponto de vista dos atacantes, uma vez que precisam de adquirir informações sobre a vítima. Normalmente, utilizam algo muito pessoal que está publicamente disponível online e facilmente acessível a qualquer pessoa. Esta informação tem muitas vezes origem em posts nas redes sociais, por vezes publicados involuntariamente por familiares da vítima, entre outros.

Por exemplo, considere-se um grupo de amigos que parte para umas férias de uma semana. Durante esta viagem, é normal que publiquem várias fotografias em várias redes sociais. Se um atacante estiver a monitorizar este grupo online e possuir

informações adicionais sobre os seus familiares, pode utilizar este conhecimento para contactar os pais de um dos amigos. Nesta altura, o atacante pode utilizar um telefone ou perfil fictício para iniciar o contacto com o seguinte contexto:






A ação esperada dos pais seria verificar duas vezes antes de enviar qualquer dinheiro. No entanto, certos elementos da história faziam sentido, criando um cenário perfeito para ser vítima de spear phishing. A nossa vida quotidiana está repleta de exemplos semelhantes, casos em que as pessoas agem impulsivamente, sem pensar bem.

Para evitar ser vítima de ataques de phishing, é essencial manter-se vigilante e adotar medidas preventivas. No caso das mensagens de correio eletrónico, as pessoas devem começar por examinar o endereço de correio eletrónico do remetente, tendo cuidado com quaisquer discrepâncias ou domínios desconhecidos que não correspondam à suposta organização. Em seguida, devem avaliar cuidadosamente o conteúdo da mensagem de correio eletrónico, prestando atenção a erros ortográfi-

cos ou gramaticais, saudações genéricas ou pedidos urgentes destinados a criar uma sensação de pânico. As organizações legítimas normalmente dirigem-se aos indivíduos pelo nome e fornecem e informações concisas. Por último, as pessoas devem evitar clicar em ligações suspeitas ou descarregar anexos sem verificar a sua legitimidade. A incorporação destas práticas aumentará a resistência pessoal contra estes esquemas. Uma estratégia para identificar hiperligações maliciosas é passar o rato sobre a hiperligação para revelar o seu destino real, garantindo que conduzem a websites legítimos.

As pessoas devem ter cuidado se a ligação redirecionar para um URL desconhecido ou suspeito. Além disso, é aconselhável digitar os URLs diretamente no browser ou utilizar os marcadores para aceder a sites de confiança.



Além disso, instale e atualize regularmente software de segurança respeitável, como programas antivírus ou anti-malware, para detetar e bloquear potenciais tentativas de phishing. Educar-se sobre técnicas de phishing também é crucial para reconhecer e evitar esses ataques. Mantenha-se informado sobre as últimas tendências de phishing, sinais de alerta comuns e táticas emergentes utilizadas pelos criminosos virtuais.

## OS INVASORES SILENCIOSOS: UMA PANORÂMICA DOS DIFERENTES TIPOS DE MALWARE

O malware refere-se a qualquer software especificamente concebido para danificar ou explorar sistemas informáticos, redes ou indivíduos. Engloba uma vasta gama de programas maliciosos, incluindo vírus, worms, trojans, spyware e ransomware. O malware pode ser distribuído através de vários meios, tais



como anexos de correio eletrónico infetados, websites comprometidos ou descarregamentos maliciosos. Uma vez instalado, o malware pode comprometer dados, roubar informações pessoais, interromper as operações do sistema ou fornecer acesso não autorizado a cibercriminosos. Compreender os diversos tipos de malware é crucial para criar estratégias de defesa eficazes. De seguida, descrevemos brevemente as diferentes categorias de malware:

- **Vírus:** Estes parasitas digitais infiltram-se nos ficheiros do hospedeiro, espalhando o seu código quando o ficheiro infetado é executado. Tal como os vírus biológicos, os vírus informáticos replicam-se, causando muitas vezes danos e caos no seu rasto.

- **Worms:** Ao contrário dos vírus, os worms funcionam de forma independente e espalham-se pelas redes, explorando vulnerabilidades para se propagarem. A sua natureza de autorreplicação permite-lhes infetar rapidamente vários sistemas.

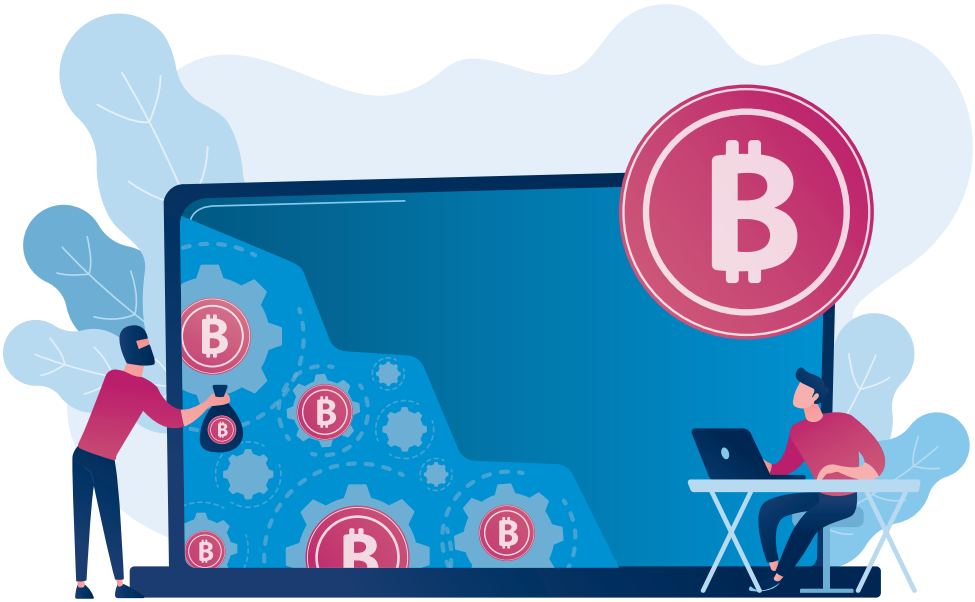
- **Trojans:** Com o nome da lendária fraude grega, os Trojans disfarçam-se de software legítimo, enganando os utilizadores para que os convidem a entrar. Uma vez lá dentro, abrem caminho para o acesso e controlo não autorizados.

- **Spyware:** Operando na sombra, o spyware recolhe silenciosamente informações sensíveis, desde palavras-passe a dados pessoais, muitas vezes com o objetivo de espionagem ou roubo de identidade.

- **Adware:** Embora menos sinistro, o adware bombardeia os utilizadores com anúncios indesejados, afetando o desempenho do sistema e a experiência do utilizador. Serve frequentemente como veículo para gerar receitas para os cibercriminosos.

- **Rootkits:** Furtivos e evasivos, os rootkits penetram profundamente no núcleo de um sistema, fornecendo acesso e controlo persistentes a agentes maliciosos. São notoriamente difíceis de detetar e remover.

- **Keyloggers:** Estas ferramentas sub-reptícias seguem e registam as teclas premidas, capturando informações sensíveis, como palavras-passe e detalhes de cartões de crédito, permitindo aos cibercriminosos roubar dados valiosos.



- **Ransomware:** Este é um tipo específico de malware que encripta os ficheiros da vítima, tornando-os inacessíveis até que seja pago um resgate. Normalmente, infiltra-se nos sistemas através de e-mails de phishing, anexos maliciosos ou kits de exploração. Uma vez ativado, o ransomware encripta ficheiros importantes e apresenta uma nota de resgate que exige o pagamento em troca da chave de desencriptação. Os ataques de ransomware têm-se tornado cada vez mais sofisticados, visando indivíduos, empresas e até infraestruturas críticas.

No passado, o malware era desenvolvido com várias vulnerabilidades, o que ajudava os profissionais de cibersegurança a reverter os danos causados. No entanto, nos últimos tempos, os cibercriminosos melhoraram a "qualidade" das suas aplicações, utilizando algoritmos conhecidos pela sua elevada resistência à desencriptação. Isto cria um cenário particularmente desafiante, uma vez que num computador comum seriam necessários milhares de milhões, ou mesmo triliões, de anos para recuperar a chave para desencriptar os ficheiros. Embora o pagamento do resgate possa parecer razoável, especialmente quando se considera o impacto da informação perdida, é frequentemente a pior decisão por várias razões. Em primeiro lugar, o indivíduo que paga o resgate indica indiretamente ao atacante que é um excelente alvo porque o pagamento é garantido. Por outras palavras, é como colocar um alvo cibernético nessa pessoa. Em segundo lugar, e não menos importante, é a falta de garantia de que a chave fornecida irá desencriptar os ficheiros. Quem pode garantir que o atacante vai atuar a sério?

O impacto do malware estende-se para além dos sistemas individuais, causando impacto a nível pessoal, empresarial e governamental.

- **Perdas financeiras:** Os incidentes relacionados com malware

podem resultar em perdas financeiras substanciais, incluindo pagamentos de resgates, custos de recuperação e potenciais sanções legais.

- **Violações de dados:** O malware compromete dados sensíveis, pondo em causa a privacidade pessoal e a confidencialidade da empresa. As consequências das violações de dados podem ser duradouras e irreparáveis.
- **Perturbação operacional:** Os ataques de ransomware podem paralisar as operações, causando períodos de inatividade e afetando a produtividade em grande escala.
- **Danos à reputação:** As organizações afetadas por incidentes de malware sofrem frequentemente danos na sua reputação, o que diminui a confiança dos clientes.
- **Preocupações com a segurança nacional:** As campanhas de malware patrocinadas pelo Estado suscitam preocupações significativas em termos de segurança nacional, visando infraestruturas s críticas e instituições governamentais.



No vasto e intrincado panorama da cibersegurança, o malware surge como um adversário formidável. As suas diversas formas e o seu impacto insidioso são um lembrete constante das ameaças digitais que enfrentamos no nosso mundo interligado. Ao compreendermos a natureza multifacetada do malware, podemos compreender melhor a necessidade de medidas robustas de cibersegurança e de vigilância permanente. À medida que a tecnologia continua a evoluir, a batalha contra o malware continua a ser um aspeto fundamental para salvaguardar o nosso futuro digital.

## DESMASCARAR WEBSITES ENGANADORES E FALSOS NOVOS

Numa era caracterizada pela acessibilidade sem precedentes da informação, surgiu um lado sinistro na paisagem digital - websites enganadores e a disseminação generalizada de notícias falsas. À medida que percorremos os intrincados caminhos da Internet, torna-se cada vez mais crucial navegar nestas águas traiçoeiras com vigilância. Mergulhando profundamente no mundo dos websites enganadores e descobrindo os efeitos perturbadores das notícias falsas, podemos descrever pontos-chave sobre a sua origem, o seu funcionamento e o seu vasto impacto.

No domínio dos websites enganosos, a ilusão de legitimidade é magistralmente tecida através de várias táticas. Estas plataformas enganosas utilizam frequentemente um design sofisticado e mímica para emular fontes genuínas, esbatendo as linhas entre autenticidade e engano. A manipulação subtil entra em jogo, tirando partido de uma linguagem persuasiva e de imagens enganadoras para explorar preconceitos cognitivos, levando os utilizadores a consumir e a partilhar conteúdos sem pensar duas vezes. A autoridade fingida contribui ainda mais para a ilusão, uma vez que os websites enganosos fabricam apoios e testemunhos, criando um verniz exterior de credibilidade que facilmente prende os leitores desprevenidos. Dentro desta intrincada teia de enganos, surge um próspero ecossistema de informações fictícias. Estas plataformas apresentam habilmente uma mistura de dados autênticos e fabricados, resultando numa distorção da realidade que semeia a confusão entre um público insuspeito.



Com intenções maliciosas no seu cerne, a disseminação de notícias falsas funciona frequentemente como uma ferramenta para enganar, manipular ou influenciar a opinião pública para promover agendas ou ideologias específicas.

Alimentada por catalisadores tecnológicos, a rápida disseminação de notícias falsas é intensificada pela viralidade das redes sociais e amplificação algorítmica. Esta dinâmica permite que a desinformação penetre em vastas audiências em prazos sem precedentes. O efeito corrosivo estende-se à erosão da confiança, uma vez que a exposição repetida a notícias falsas corrói a confiança do público nas instituições estabelecidas, cultivando uma atmosfera de ceticismo que pode potencialmente diminuir a credibilidade da informação fatual. A influência das notícias falsas não se fica por aqui, estende-se à formação das crenças

individuais e aos processos coletivos de tomada de decisões, sublinhando a urgência de contrariar o seu impacto insidioso.

As ramificações globais são inegáveis, uma vez que as notícias falsas atravessam fronteiras, exercendo a sua influência nas relações internacionais, moldando as respostas de saúde pública e inflamando as tensões sociais com consequências de longo alcance.

O impacto dos websites enganadores e das notícias falsas ultrapassa em muito o domínio da paisagem digital, deixando uma marca indelével em vários aspetos da sociedade. A influência das notícias falsas no discurso público e nas crenças individuais pode levar à erosão da confiança nas instituições estabelecidas, criando um ambiente de ceticismo que mina os próprios fundamentos de uma cidadania bem informada. Os websites enganadores, com a sua mímica artística de legitimidade, contribuem para esta erosão ao esbaterem as linhas entre facto e ficção, deixando os indivíduos vulneráveis à manipulação. Estes são fundamentais para apoiar outros ataques, como o phishing. Além disso, a rápida disseminação de informações falsas através das redes sociais amplifica o impacto, uma vez que as histórias sensacionalistas e as narrativas enganosas se espalham como um incêndio, potencialmente incitando à agitação e exacerbando as tensões sociais. Consequentemente, as profundas implicações das notícias falsas e dos websites enganosos estendem-se a domínios como o discurso político, a coesão social e a saúde pública, sublinhando a necessidade urgente de literacia mediática, pensamento crítico e envolvimento digital responsável para navegar nesta paisagem complexa e em evolução.

BACK 2 BASICS

3

UM MANUAL DE CIBERSEGURANÇA

# CIBER-HIGIENE: MELHORES PRÁTICAS

# **CIBER-HIGIENE:** MELHORES PRÁTICAS

No mundo digital atual, em que as nossas vidas estão interligadas com a tecnologia de formas sem precedentes, o conceito de ciber-higiene surgiu como uma pedra angular fundamental de um comportamento online responsável e seguro. Tal como damos prioridade à higiene pessoal para manter o nosso bem-estar físico, a adoção de práticas sólidas de ciber-higiene é essencial para preservar a nossa saúde digital e para nos protegermos contra um cenário de ciberameaças em rápida evolução. Esta secção do documento aprofunda o domínio da ciber-higiene, apresentando um conjunto abrangente de melhores práticas que permitem às pessoas navegar no domínio digital com confiança, resiliência e maior consciência do panorama da cibersegurança. Desde o reforço das palavras-passe até ao cultivo de um olhar perspicaz para as tentativas de phishing, este capítulo serve de guia para elevar o seu bem-estar digital e promover uma experiência online mais segura e protegida.

## DEFINIÇÃO DE CIBER-HIGIENE

Num mundo cada vez mais interligado, onde as nossas vidas estão interligadas com a tecnologia, tornou-se essencial dar prioridade à cibersegurança. Tal como praticamos a higiene pessoal para proteger o nosso bem-estar físico, adotar bons hábitos de ciber-higiene é crucial para salvaguardar a nossa vida digital. Mas o que é exatamente a ciber-higiene?

A ciber-higiene refere-se a um conjunto de boas práticas e hábitos que os indivíduos e as organizações devem adotar para garantir a segurança e a integridade do seu ambiente digital. Engloba um vasto leque de ações e comportamentos que contribuem para a prevenção de ciberameaças, tais como infeções por malware, violações de dados e roubo de identidade.

Ser ciber-higiénico é da maior importância no panorama digital atual. As ciberameaças continuam a evoluir e a aumentar em sofisticação, apresentando riscos significativos tanto para os indivíduos como para as organizações. Ao praticarmos uma boa ciber-higiene, podemos proteger-nos a nós próprios e às nossas informações sensíveis de agentes maliciosos de forma proativa. Isso ajuda a evitar potenciais consequências, como roubo de identidade, perdas financeiras e danos à reputação. Manter palavras-passe fortes, atualizar regularmente o software e ter cuidado com as tentativas de phishing são apenas alguns exemplos de práticas de ciber-higiene que podem reduzir significativamente a probabilidade de ser vítima de ciberataques. Além disso, ser ciber-higiénico não só salvaguarda o nosso próprio bem-estar digital, como também contribui para a segurança coletiva do mundo interligado, promovendo um ambiente online mais seguro para todos.



## RECOMENDAÇÕES PARA SE MANTER SEGURO ONLINE

Atualizar regularmente o seu software é semelhante a cuidar de um jardim digital. Os sistemas operativos, as aplicações e o software de segurança evoluem para resolver novas vulnerabilidades e melhorar a proteção. Um sistema atualizado é a sua linha da frente de defesa contra as ciberameaças, garantindo

que os potenciais pontos de entrada para os hackers estão fechados. Ao ativar as atualizações automáticas ou ao verificar consistentemente a existência de atualizações, está a impedir proativamente as tentativas dos cibercriminosos de explorarem software desatualizado, protegendo o seu jardim digital. Adotar a prática de atualizações de software é um passo poderoso para uma existência digital mais segura. Com cada atualização, os seus dispositivos são equipados com os mais recentes patches de segurança, tornando exponencialmente mais difícil para os ciberataques violarem as suas defesas. Estas atualizações não se limitam a repelir ameaças iminentes - cultivam uma mentalidade proativa que reforça a resiliência da sua cibersegurança. Ao dedicar alguns minutos a atualizações regulares, está a contribuir para um ambiente online mais seguro para si e para os outros, demonstrando o poder da vigilância coletiva.



No domínio da cibersegurança, uma palavra-passe robusta é a fortaleza virtual do utilizador, protegendo-o contra o acesso não autorizado. Criar uma palavra-passe forte não é uma mera tarefa, é uma arte. Ao entrelaçar uma sinfonia de letras, números, símbolos e letras maiúsculas e minúsculas, é possível compor uma frase-passe que seja simultaneamente formidável e difícil de decifrar. Cada conta merece a sua própria palavra-passe. Considere a possibilidade de recorrer à ajuda de um gestor de palavras-passe de confiança, aliviando os utilizadores do fardo mental de recordar códigos complexos e garantindo que as suas chaves digitais permanecem armazenadas de forma segura. Mais detalhes sobre este tópico são discutidos nas secções seguintes.

No meio das correntes digitais, os esquemas de phishing são os remoinhos enganadores que procuram apanhar vítimas desprevenidas. A vigilância é a sua bússola; antes de sucumbir à sedução de um e-mail, examine a sua autenticidade. Passar o

rato sobre as hiperligações para discernir o seu verdadeiro destino é um ato pequeno, mas potente, que o pode proteger do precipício de uma potencial violação. Quando um e-mail invoca urgência, faça uma pausa e tenha cuidado. Este é o modus operandi dos cibercriminosos que procuram tirar partido de decisões precipitadas. Confie nos seus instintos e verifique a identidade do remetente através dos canais de comunicação estabelecidos, dissuadindo o engodo astuto de uma expedição de phishing. O ceticismo, juntamente com pensamento crítico,

forma um escudo indomável contra a maré traiçoeira das tentativas de phishing. Pense em si como um detetive cibernético que investiga pistas e descobre a verdade. Ao adotar uma mentalidade vigilante e cautelosa online, transforma-se num navegador experiente, navegando nas águas traiçoeiras do engano com um discernimento inabalável. Lembre-se de que um momento de ceticismo pode evitar horas de controlo de danos, ilustrando o poder de uma mentalidade vigilante e perspicaz.

As redes Wi-Fi públicas oferecem o atrativo de uma conetividade sem falhas, mas escondem frequentemente riscos ocultos. O envolvimento com essas redes exige uma abordagem cautelosa; trate-as como mercados lotados onde as informações pessoais estão expostas. As atividades que envolvem dados sensíveis, tais como a banca online ou a transferência de documentos confidenciais, devem ser reservadas para ligações seguras e privadas. A utilização criteriosa de uma Rede Privada Virtual (VPN) atua como uma capa digital, encriptando os seus dados e protegendo-os de olhares indiscretos, tornando-o imune a potenciais espiões. No domínio da segurança da rede, a consciência e a prudência são as suas estrela-guia. Considere as redes Wi-Fi públicas como praças movimentadas repletas de estranhos, onde os seus segredos podem ser ouvidos por qualquer transeunte. A máscara digital de uma VPN acrescenta uma camada extra de proteção, assegurando que sua pegada digital permanece escondida de curiosos. Ao adotar estas práticas, estará a dotar-se das ferramentas necessárias para percorrer o mundo virtual com confiança, sabendo que as suas atividades online estão protegidas contra potenciais adversários.

Embora as estratégias acima mencionadas contribuam para aumentar a segurança online, vamos analisar uma lista abrangente das dez melhores práticas para promover a resiliência contra as ciberameaças.

1. **Palavras-passe fortes: Crie palavras-passe únicas e fortes para cada conta.**
2. **Autenticação multi-fator (MFA): Utilizar a MFA sempre que disponível.**
3. **Atualizações regulares: Mantenha o software e os dispositivos atualizados.**
4. **Seja cauteloso online: Esteja atento a mensagens de correio eletrónico e ligações suspeitas.**
5. **Evitar a rede Wi-Fi pública: Evite atividades sensíveis em redes Wi-Fi públicas.**
6. **Cópia de segurança dos dados: Faça regularmente cópias de segurança de ficheiros importantes.**
7. **Definições de privacidade: Ajustar as definições de privacidade das redes sociais.**
8. **Dispositivos seguros: Bloqueie os dispositivos com palavras-passe fortes.**
9. **Pense antes de clicar: Tenha cuidado com os descarregamentos e as ligações.**
10. **Manter-se informado: Mantenha-se informado sobre as ameaças à cibersegurança.**

## ATENUAÇÃO E RECUPERAÇÃO

Os ciberataques tornaram-se uma forma predominante e sofisticada de cibercrime, causando danos significativos às organizações em todo o mundo. Para minimizar o seu impacto e recuperar eficazmente de tais incidentes, é crucial seguir um conjunto bem definido de diretrizes. Algumas das melhores práti-

cas para implementar uma estratégia de cópia de segurança sólida para proteger os seus dados valiosos são as seguintes:

- **Isolamento imediato:** O primeiro passo para conter um ataque, por exemplo, um ataque de ransomware, é desligar todos os dispositivos infetados, como computadores, portáteis ou tablets, de quaisquer ligações de rede, incluindo com fios, sem fios e móveis. Em casos graves, considere desligar o Wi-Fi, desativar as ligações de rede principais e desligar a Internet, se necessário.

- **Redefinir credenciais:** A reposição das credenciais, especialmente as palavras-passe das contas de administrador e de sistema, é crucial para evitar mais acessos não autorizados. No entanto, tenha cuidado para evitar ficar sem acesso a sistemas essenciais necessários para a recuperação.

- **Limpar com segurança os dispositivos infetados:** No caso de ataques de malware, para erradicar completamente o problema, limpe com segurança os dispositivos infetados e reinstale o sistema operativo. Este passo garante que todos os vestígios do malware são removidos, proporcionando um quadro limpo para a recuperação.

- **Verificar a integridade da cópia de segurança:** Antes de restaurar a partir de uma cópia de segurança, certifique-se de que esta está livre de qualquer malware. Apenas prossiga com o processo de restauro se tiver a certeza de que tanto a cópia de segurança como o dispositivo onde a está a instalar estão limpos.

- **Ligar a uma rede limpa:** Para transferir, instalar e atualizar o sistema operativo e todos os outros softwares, ligue os dispositivos a uma rede limpa. Isto garante que nenhum ficheiro infetado é transferido inadvertidamente durante o processo de recuperação

- **Instalar e atualizar o software antivírus:** Proteja os seus sistemas de futuros ataques instalando, atualizando e executando software antivírus fiável. A verificação regular dos seus dispositivos com as definições antivírus mais recentes, pode ajudar a identificar e eliminar quaisquer infeções remanescentes.

- **Ligação à rede:** Depois de ter tomado as precauções necessárias e assegurado a integridade dos seus sistemas, volte a ligar-se à sua

rede. No entanto, monitorize de perto o tráfego de rede e efetue análises antivírus periódicas para detetar quaisquer sinais de malware persistente.



## CONCEÇÃO DE UMA ESTRATÉGIA DE SALVAGUARDA SÓLIDA

A melhor solução para aumentar a segurança no ciberespaço é a prevenção de potenciais problemas.  Para estar preparado para as ciberameaças, recomenda-se a utilização de cópias de segurança, nomeadamente através da implementação de uma política de cópias de segurança sólida que privilegie as cópias de segurança regulares dos ficheiros críticos. A importância destes ficheiros pode variar para cada utilizador ou organização, pelo que é essencial avaliar e dar prioridade às suas necessidades específicas. As recomendações são as seguintes:

- **Backups offline e fora do local:** Para proteger as suas cópias de segurança contra ataques, crie cópias de segurança offline armazenadas numa localização diferente, de preferência externamente. Considere a utilização de serviços de armazenamento na nuvem explicitamente concebidos para cópias de segurança seguras. Diversifique as soluções de backup e os locais de armazenamento para minimizar o risco de perda de dados. A adesão à estratégia de backup 3-2-1 garante redundância e resiliência.

- **Desligue os dispositivos de cópia de segurança:** Evite manter discos rígidos externos contendo cópias de segurança permanentemente ligadas à sua rede. No caso de um ataque, se estes dispositivos estiverem ligados, podem ser afetados. Por exemplo, os operadores de ransomware visam frequentemente dispositivos de cópia de segurança ligados, tornando a recuperação de dados mais difícil. Desligá-los quando não estão a ser utilizados atenua este risco.

- **Proteger versões anteriores:** Certifique-se de que o fornecedor de serviços na nuvem escolhido protege as versões anteriores dos backups. Alguns serviços sincronizam automaticamente os ficheiros, substituindo potencialmente versões não encriptadas por cópias encriptadas. A manutenção de várias versões de backups garante a disponibilidade de dados não corrompidos para recuperação.

- **Atualizar regularmente os servidores de cópia de segurança:** Atualize regularmente os seus servidores de cópia de segurança para resolver quaisquer vulnerabilidades que possam ser exploradas por atacantes. Identificar e corrigir proativamente os pontos fracos pode aumentar a segurança e a resiliência da sua infraestrutura de cópia de segurança.

- **Verificar dispositivos limpos:** Antes de iniciar o processo de restauro, certifique-se de que as suas cópias de segurança estão apenas ligadas a dispositivos limpos conhecidos. Além disso, analise as soluções de backup em busca de malware para evitar a reintrodução inadvertida de arquivos infetados na rede.

Ao seguir as diretrizes recomendadas e implementar uma estratégia de cópia de segurança robusta, pode minimizar significativamente o impacto de um surto de ransomware e garantir um processo de recuperação rápido e eficaz. Atualizar e testar regularmente as cópias de segurança de dados e os procedimentos de recuperação é crucial para garantir que, no caso de um ciberataque, estes recuperam eficazmente os seus dados e minimizam o tempo de inatividade.

BACK 2 BASICS

4

UM MANUAL DE CIBERSEGURANÇA

# GESTÃO DE PALAVRAS-PASSE DE AUTOPROTEÇÃO

# GESTÃO DE PALAVRAS-PASSE DE AUTOPROTEÇÃO

A gestão eficaz de palavras-passe é um aspeto fundamental da autoproteção no panorama digital. Inclui não só a criação de palavras-passe fortes e únicas, mas também a sua gestão diligente e revisão regular. Isto implica a adoção de estratégias como a utilização de um gestor de palavras-passe fiável para armazenar e organizar diferentes palavras-passe, garantindo que cada conta tem uma palavra-passe distinta para evitar que uma violação numa conta comprometa outras contas. É igualmente crucial atualizar regularmente as palavras-passe, especialmente para contas sensíveis, e estar atento a potenciais ataques de phishing. A autoproteção estende-se ao conhecimento das características de segurança fornecidas pelas diferentes plataformas, como a autenticação de dois fatores, que acrescenta uma camada adicional de segurança. Igualmente importante é a consciência da pegada digital de cada um e dos potenciais riscos envolvidos na partilha de informações pessoais online. Mantendo-se informadas e adotando práticas sólidas

de gestão de palavras-passe, as pessoas podem melhorar significativamente a sua segurança online e proteger as suas informações pessoais e sensíveis contra o acesso não autorizado.

## RISCOS DE UMA PALAVRA-PASSE FRACA

Antes de definir o que são palavras-passe fracas e o impacto da sua fraqueza, precisamos de compreender como é que os atacantes podem descobrir as nossas credenciais. Existem diferentes formas de obter as credenciais de um indivíduo, assumindo que estas não foram fornecidas num ataque de phishing. Um atacante pode intercetar a comunicação, realizando o que é conhecido como um ataque Man-In-the-Middle. Com a popularização das comunicações HTTPS, estes ataques tornaram-se menos eficazes, pelo que não os discutiremos mais neste documento. No entanto, outra técnica é o roubo de bases de dados explorando as vulnerabilidades existentes nas aplicações Web.

Esta última questão continua a ser uma preocupação e é complexa de controlar. Quando um atacante consegue roubar uma base de dados privada que contém credenciais, estas são armazenadas de três formas:

1. **como texto livre (menos comum nos dias de hoje);**
2. **utilizando um hash, que é uma técnica que converte a palavra-passe em algo diferente utilizando algoritmos irreversíveis; e**
3. **utilizando um hash com sal, que é mais robusto.**

O processo de hashing de uma palavra-passe baseia-se em funções de digestão. O objetivo destas funções é a criação de

um conjunto definido de bits que representam a informação original. Estas seguem alguns princípios, um dos quais define que usando um hash não deve ser possível obter a informação original que criou o tal hash.

Por conseguinte, um atacante que tenha um hash de uma palavra-passe não pode obter a palavra-passe diretamente.

Os hashes iniciais foram concebidos para serem seguros, mas descobertas posteriores revelaram certas técnicas capazes de quebrar alguns hashes quase instantaneamente. Este facto levou ao desenvolvimento de algoritmos de hashing mais avan-



çados e seguros. A vulnerabilidade das palavras-passe é mais frequentemente exposta em cenários como:

- **Armazenadas em bases de dados comprometidas:** Quando as palavras-passe são armazenadas em bases de dados que não estão adequadamente protegidas, tornam-se suscetíveis de acesso não autorizado e de potenciais violações.
- **Armazenadas em texto simples:** O armazenamento de palavras-passe em texto simples, sem qualquer forma de encriptação, torna-as alvos fáceis para os cibercriminosos que obtêm acesso ao sistema de armazenamento.
- **Representado usando hashes:** Embora os hashes sejam utilizados

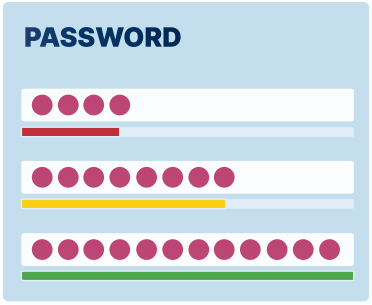
para aumentar a segurança, alguns algoritmos de hashing foram considerados vulneráveis, tornando as palavras-passe suscetíveis de ataques.

- **Intercetadas na comunicação:** As palavras-passe podem ser intercetadas durante a sua transmissão através de redes, especialmente se o canal de comunicação não for encriptado de forma segura.
- **Redes desprotegidas:** A utilização de palavras-passe em redes desprotegidas ou públicas aumenta o risco de estas serem capturadas por agentes maliciosos, uma vez que estas redes não dispõem frequentemente de medidas de segurança suficientes.

A compreensão destas vulnerabilidades comuns sublinha a importância de uma gestão robusta das palavras-passe e de práticas de segurança para proteger informações pessoais e sensíveis.



## DEFINIR PALAVRAS-PASSE FORTES




A definição de palavras-passe fortes é crucial para proteger as suas contas online e informações pessoais. Eis algumas orientações importantes para criar palavras-passe fortes:

- **O comprimento é importante:** Procure ter pelo menos 12 a 16 caracteres. As palavras-passe mais longas são geralmente mais seguras.
- **Utilizar uma mistura de personagens:** Incorpore uma variedade de personagens na sua palavra-passe, incluindo:
  - **Letras maiúsculas (A-Z)**
  - **Letras minúsculas (a-z)**
  - **Números (0-9)**
  - **Caracteres especiais (por exemplo, !, @, #, $)**

- **Evitar padrões previsíveis:** Não utilize caracteres sequenciais ou repetitivos (como "12345" ou "aaaaa"). Estes são mais fáceis de adivinhar para os atacantes**.**
- **Sem informações pessoais:** Evite utilizar informações fáceis de adivinhar, como o seu nome, data de nascimento ou palavras comuns. Estas podem ser frequentemente encontradas nas redes sociais ou adivinhadas.
- **Palavras ou frases incomuns:** Considere utilizar uma palavra ou frase aleatória e invulgar. Melhor ainda, junte várias palavras não relacionadas.
- **Considere uma frase-chave:** Uma frase-senha é uma sequência de palavras ou uma frase. É mais fácil de lembrar e pode ser bastante longa, tornando-a mais segura. Por exemplo, "BlueCoffeeMugOnDesk!".
- **Use substituições não padronizadas:** Se utilizar palavras ou frases, tente fazer substituições criativas, como utilizar um "3" em vez de um "E" ou um "$" em vez de um "S".
- **Teste a sua palavra-passe:** Muitas ferramentas online permitem-lhe verificar a força da sua palavra-passe (dica: não utilize a sua palavra-passe real). Podem dar-lhe uma ideia de quão fácil ou difícil seria decifrá-la.
- **Alterar as palavras-passe regularmente:** Embora nem sempre seja necessário, especialmente se utilizar uma palavra-passe única e forte, a alteração regular das palavras-passe pode ser benéfica, especialmente para contas sensíveis.
- **Mantenha-se informado:** Esteja a par das melhores práticas atuais para a segurança das palavras-passe, uma vez que as recomendações podem evoluir com a evolução da tecnologia e das ameaças à segurança.

Ao seguir estas diretrizes, pode criar palavras-passe fortes e eficazes que ajudam a proteger as suas informações digitais. Lembre-se de que a força de uma palavra-passe reside fre-



quentemente não só na sua complexidade, mas também na sua singularidade e imprevisibilidade.

## RECOMENDAÇÕES PARA A GESTÃO DA PALAVRA-PASSE

Gerir as palavras-passe de forma eficaz é crucial para manter a segurança e a privacidade online. Seguem-se algumas recomendações para gerir as palavras-passe:

- **Utilize palavras-passe fortes e únicas:** Cada uma das suas contas deve ter uma palavra-passe única. As palavras-passe fortes incluem normalmente uma mistura de letras (maiúsculas e minúsculas), números e caracteres especiais. Evite palavras e frases comuns.
- **Utilize um gestor de palavras-passe:** Os gestores de palavras-

passe podem gerar e armazenar palavras-passe complexas por si. Mantêm as suas palavras-passe seguras e acessíveis através de uma palavra-passe mestra. Isto reduz o fardo de se lembrar de várias palavras-passe fortes.

- **Autenticação de dois fatores (2FA):** Sempre que possível, ative a 2FA. Isto adiciona uma camada extra de segurança ao exigir uma segunda forma de identificação para além da sua palavra-passe, como um código de mensagem de texto ou uma notificação de aplicação.

- **Atualizar regularmente as palavras-passe:** Altere as suas palavras-passe regularmente, especialmente para contas sensíveis como correio eletrónico, serviços bancários e redes sociais. No entanto, não são necessárias alterações frequentes se utilizar palavras-passe fortes e únicas e não tiver sofrido uma violação.

- **Cuidado com os ataques de phishing:** Tenha cuidado com o local onde introduz a sua palavra-passe. Os ataques de phishing muitas vezes induzem as pessoas a fornecerem as suas palavras-passe em websites falsos. Verifique sempre o URL do website antes de introduzir as suas credenciais.

- **Perguntas de segurança:** Escolha perguntas e respostas de segurança que não sejam fáceis de adivinhar. Por vezes, informações como o nome de solteira da sua mãe ou a sua primeira escola podem ser encontradas online ou adivinhadas.

- **Monitorizar contas para detetar violações:** Utilize serviços que o alertem se o seu e-mail ou palavra-passe tiverem sido comprometidos numa violação de dados. Isto permite-lhe alterar a sua palavra-passe imediatamente.

- **Evitar a utilização de informações pessoais:** Evite utilizar informações facilmente acessíveis como o seu nome, data de nascimento ou sequências simples como "1234" nas suas palavras-passe.

- **Não partilhar palavras-passe:** Evite partilhar as suas palavras-passe com outras pessoas. Se tiver de partilhar uma palavra-passe, altere-a o mais rapidamente possível.

- **Informações de recuperação de backup:** Certifique-se de que as

informações de recuperação da sua conta estão atualizadas. Isto inclui o seu endereço de correio eletrónico ou número de telefone utilizado para recuperar as suas contas em caso de esquecimento da sua palavra-passe.

A chave para uma gestão eficaz das palavras-passe é uma combinação de palavras-passe fortes e únicas, a utilização de um gestor de palavras-passe fiável e a vigilância contra as ameaças à segurança.

BACK 2 BASICS

# 5

UM MANUAL DE CIBERSEGURANÇA

# CONCLUSÃO

# CONCLUSÃO



Ao longo deste manual, explorámos a importância crítica da cibersegurança e aprofundámos as várias melhores práticas e estratégias de proteção contra as ciberameaças comuns. Ao concluirmos a nossa viagem, vamos recapitular as principais conclusões e sublinhar a importância de implementar estas práticas nas nossas vidas pessoais e profissionais.

Antes de mais, é fundamental manter uma boa higiene cibernética. Ao atualizar regularmente o software, utilizar palavras-passe fortes e únicas e ter cuidado ao ligar-se a redes Wi-Fi públicas, os indivíduos podem reduzir significativamente o risco de serem vítimas de ciberataques. As organizações também devem dar prioridade à ciber-higiene, implementando medidas de segurança robustas, realizando auditorias de segurança regulares e educando os seus funcionários sobre práticas online seguras.

Em conclusão, a principal conclusão deste manual é que a cibersegurança é uma responsabilidade coletiva. Ao implementar as melhores práticas aqui discutidas, os indivíduos e as organizações podem reduzir significativamente o risco de serem vítimas de ciberameaças e proteger a sua informação sensível, os seus ativos financeiros e a sua reputação. A cibersegurança não é um esforço único, mas um compromisso permanente. Requer educação, consciencialização e adaptação contínuas para se manter um passo à frente dos cibercriminosos.

Lembremo-nos de que o nosso mundo digital está em constante evolução, tal como as táticas e técnicas utilizadas pelos ciber-atacantes. Se nos mantivermos vigilantes, informados sobre as ameaças que surgem, e adaptando as nossas defesas em conformidade, podemos navegar no panorama digital com segurança e confiança.

Juntos, podemos construir um ecossistema digital mais seguro e resistente, para benefício de todos.


universidade
de aveiro

BIO
LIVING

HELLENIC
REPUBLIC
UNIVERSITY
OF MACEDONIA

gri