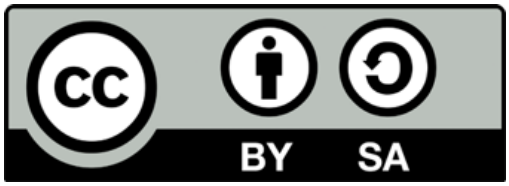
ICT4D Collective

Utilizando as tecnologias digitais de forma segura, inteligente e protegida:
um breve guião para as pequenas organizações da sociedade civil

Tim Unwin

Em nome do Coletivo ICT4D
https://ict4d.org.uk

Versão 6
maio de 2025



ICT4D Collective

Não se trata de uma questão de "se", mas de "quando" a sua organização sofrerá um ataque cibernético de algum tipo.

Isto pode acontecer directamente através dos seus próprios ambientes digitais ou pode ser afectado por um ataque a uma organização com a qual trabalhas. Por conseguinte, é essencial tomar todas as precauções possíveis para manter o teu pessoal e aqueles com quem trabalha em segurança. As tecnologias digitais podem ser utilizadas para trazer muitos benefícios às organizações, mas é essencial atenuar os danos para que os benefícios possam ser concretizados.

É seguro? É inteligente? Está protegido?

Este breve guião foi concebido para fornecer às pequenas organizações da sociedade civil (especialmente às que têm poucos recursos) conselhos básicos sobre como utilizar a tecnologia digital de forma segura, inteligente e protegida/privada. Não pretende ser exaustivo nem altamente técnico, mas centra-se em aspectos que devem ser seguidos por todas as organizações da sociedade civil, independentemente da sua capacidade técnica ou financeira. A cibersegurança básica é essencial e, com a evolução de tecnologias como a IA e a computação quântica, as ameaças só vão piorar. A adopção destas práticas fundamentais não impedirá necessariamente que seja atacado, mas deverá reduzir as hipóteses e o impacto de tais ataques e ajudá-lo-á a voltar a estar conectado (online) o mais rapidamente possível.

Como é que reagiria ou evitaria os seguintes cenários?

> Você é o fundador de uma organização da sociedade civil que oferece refúgio a mulheres vítimas de violência doméstica. O seu Website mostrava fotografias de algumas das mulheres que se encontravam num dos seus abrigos e foram partilhadas fotografias nas redes sociais. Um dia, um grupo de jovens, incluindo um homem que já tinha agredido uma das mulheres, atacou as pessoas que se encontravam no abrigo e matou duas das mulheres.

> Você dirige uma grande organização que apoia crianças em risco de viver e trabalhar nas ruas e mantém um registo nos seus computadores dos dados de contacto de todo o seu pessoal, das pessoas com quem trabalha e das suas famílias. Um dia, ao chegar ao trabalho, abre o computador principal da organização e descobre que não consegue aceder aos dados e que aparece uma imagem e um texto de grandes dimensões no seu ecrã a dizer que os seus dados serão partilhados abertamente na Internet, a não ser que pague um resgate avultado que levaria a sua organização à falência e arruinaria a sua reputação.

As notas de orientação que se seguem são tão simples e claras quanto possível, com uma utilização mínima de linguagem técnica. As recomendações a vermelho são consideradas essenciais; as a azul são altamente recomendadas.

ICT4D Collective

O que é mais importante para si? Planeie para proteger.

Tal como os exemplos acima sugerem, deve começar por pensar quais os dados ou informações que mais precisa de proteger nos seus sistemas digitais e, em seguida, criar um plano para o ajudar a atingir esse objectivo. Para algumas organizações que trabalham em questões sensíveis com pessoas muito vulneráveis, isso pode ser garantir que as identidades dessas pessoas são sempre mantidas o mais seguras e inacessíveis possível a terceiros. Para outras, pode ser a possibilidade de comunicar sempre com os membros do pessoal no terreno e, para outras ainda, pode ser a garantia de que os seus arquivos históricos são preservados para o futuro. Tem de pensar na informação *que* tem, *porque* a tem e *se precisa mesmo de a ter online*. Se começar simplesmente por identificar as suas cinco principais prioridades e começar a tentar garantir a sua protecção, já terá dado um passo significativo. No entanto, nunca se esqueça de ter também um plano de backup não digital, para que possa continuar a prestar os seus serviços e a fazer o seu trabalho sem ter de utilizar os seus sistemas digitais, caso seja necessário.

Paralelamente, crie uma cultura de cibersegurança entre todo o seu pessoal e aqueles com quem trabalha. Deve envolvê-los na tomada de decisões para que possam contribuir com as suas ideias e apropriar-se das orientações e práticas resultantes. O seu plano deve também centrar-se no apoio colectivo (ajudar os outros a adoptar boas práticas de ciber-higiene) em vez de medidas punitivas individuais (culpar alguém por uma violação de segurança). Para tal, pode ser muito útil ter cartazes e slogans adequados e relevantes sobre cibersegurança expostos de forma proeminente nos seus escritórios e espaços públicos (ver anexo com exemplos e outros recursos). Isto ajuda a criar uma cultura de cibersegurança muito importante entre a sua equipa e pode, além disso, sensibilizar as pessoas que visitam os seus escritórios para estas questões.

Conheça os tipos de ataque que poderá encontrar.

Existem inúmeros tipos de ciberataques e fraudes que a sua organização pode encontrar, mas alguns dos mais susceptíveis de afectar as organizações da sociedade civil são:

- *Falsificações profundas*: utilização de imagens, áudio ou vídeo gerados por IA para prejudicar a reputação ou influenciar a opinião pública.
- *Roubo de identidade*: quando um atacante acede à sua identidade/credenciais e se faz passar por si. É difícil de detectar porque o atacante imita os seus comportamentos normais e palavras-passe (password).
- *Malware*: termo genérico utilizado para se referir a qualquer programa ou código malicioso criado com a intenção de causar danos a um computador, rede ou servidor.
- *Phishing*: um ataque que utiliza o correio eletrónico, SMS, telefone, redes sociais ou técnicas de engenharia social para o levar a partilhar informações sensíveis, como palavras-passe ou números de conta.
- *Ransomware*: malware que encripta os seus dados e o atacante exige um pagamento para restaurar o seu acesso aos ficheiros e à rede. Esta é actualmente uma das formas mais frequentes de ataque e ameaça muitos tipos diferentes de organizações. Um ataque de ransomware de duplo risco é quando o atacante também ameaça publicar os seus dados online.
- *Chantagem Sexual online*: extorquir dinheiro ou favores sexuais a alguém através da ameaça de revelar imagens ou provas do seu comportamento sexual online.

- *Spoofing*: uma técnica através da qual um atacante se disfarça de uma fonte conhecida ou de confiança (como um amigo ou um banco). Ao fazê-lo, consegue interagir consigo e aceder aos seus sistemas ou dispositivos com o objectivo final de roubar informações, extorquir dinheiro ou instalar malware ou outro software nocivo num dispositivo.
- A fraude *SIM-Swap (troca de cartão de SIM)*, em que um criminoso engana a tua rede móvel para transferir o teu número para um cartão SIM na posse do criminoso, que depois utiliza para receber as tuas senhas de segurança de uso único e, assim, aceder às tuas contas.

Estes variam consideravelmente em frequência, dependendo em parte do tipo da sua organização e do contexto local. No entanto, o risco de fraude através de falsificação é provavelmente o mais comum que poderá encontrar (muitas vezes conhecido como *Business Email Compromise* – comprometimento do seu email instituicional). Isto acontece mais frequentemente quando um e-mail ou mensagem falsificadas pedem a transferência de dinheiro, e a principal protecção é processual e não técnica. Você deve criar uma cultura básica em que os pedidos invulgares são sempre tratados com desconfiança e garantir que os processos correctos de autorização de pagamento estejam sempre em vigor.

Lembre-se que estão sempre a ser desenvolvidas novas formas de fraude e ataques. Por conseguinte, é muito importante manter a sua organização actualizada e actualizar regularmente as suas orientações em resposta a quaisquer novos tipos de ameaças.

O seu pessoal: o maior risco e a primeira linha de defesa

A maioria dos ataques a sistemas digitais é causada por "erro humano", em que alguém clica acidentalmente numa ligação (link) que o leva para uma página falsa. É cada vez mais difícil detectar estas fraudes e o pessoal deve ser encorajado a considerar qualquer mensagem inesperada como sendo potencialmente perigosa.

- Nomeie um membro do pessoal de confiança (e com conhecimentos técnicos) como responsável pela segurança digital global, independentemente da dimensão da sua organização, e assegure-se de que ele
  - Tenha uma formação adequada (com actualizações regulares).
  - Crie um plano de resposta a incidentes e de recuperação que inclua, no mínimo
    - Os sistemas que são críticos e importantes para a organização.
    - Quem deve contactar ou comunicar o incidente para obter assistência.
  - Conheça os pormenores dos protocolos nacionais relevantes da CSIRT (*Computer Security Incident Response Team* - Equipa de resposta a incidentes de segurança informática;; ou CERT *Computer Emergency Response/Readiness Team - Equipa de resposta/preparação para emergências informáticas*). Embora estes protocolos se destinem geralmente a organizações de maior dimensão, têm frequentemente bons conselhos e sugestões.
  - Partilhe com todo o pessoal actualizações regulares sobre as ameaças mais recentes.
  - Incentive uma atmosfera de denúncia aberta e não de culpabilização.

    - Apresente regularmente relatórios sobre a cibersegurança ao Director Executivo/Conselho de Administração ou equivalente.
- Certifique-se de que todo o pessoal utiliza nomes de utilizador e palavras-passe complexos e únicos para todos os seus diferentes inícios de sessão e aplicações.
    - Todas as palavras-passes devem ter pelo menos 12 caracteres e, de preferência, utilizar números, caracteres minúsculos, caracteres maiúsculos e símbolos.
        - Embora possam ser difíceis de memorizar, imprimi-las em papel e guardá-las num local seguro pode ser mais seguro do que guardá-las numa pasta no seu dispositivo.
        - As palavras-passe devem ser regularmente actualizadas e imediatamente alteradas após o anúncio de qualquer violação de dados para a qual possa ter um login.
    - Uma abordagem alternativa à criação de palavras-passe é utilizar três palavras aleatórias, como máça fenda oceano, e criar uma única palavra-passe "máçafendooceano" a partir delas (novamente com mais de 12 caracteres). Isto combina a facilidade de memorização com o comprimento e, para criar diversidade, pode utilizar as palavras numa ordem diferente para fins diferentes, como em "oceanomáçafendo".
- Exigir múltiplas autenticações para todos os logins, tanto relacionados com a organização como com a sua vida pessoal (pelo menos duplas, 2FA, ou seja, dois sistemas ou factores/categorias diferentes, como um dispositivo móvel e um computador portátil, ou utilizando também o reconhecimento facial, para autenticar o acesso a um dispositivo; MFA é a autenticação multifactor; note que 2SV é a verificação em duas etapas, que exige duas etapas, mas normalmente da mesma categoria de verificação; não confie apenas em números de telefone que podem ser sujeitos a SIM-Swaps e utilizados para aceder às suas contas)
    - Estão disponíveis várias aplicações para activar a autenticação dupla, incluindo
        - Duo Mobile (Cisco)
        - Microsoft Authenticator
        - Google Authenticator
- Disponibilize formação/actualizações anuais sobre cibersegurança a todo o pessoal e incentive-o a assumir a responsabilidade pela sua própria segurança online, tanto no trabalho como na sua vida pessoal.
- Não permita a utilização de dispositivos e aplicações relacionados com o trabalho para uso pessoal do pessoal.
- Assegure-se de que, quando o pessoal ou os utilizadores deixam a sua organização para outro emprego, as suas contas são desactivadas ou terminadas e os dados pessoais são removidos dos seus sistemas.
- Os voluntários e o pessoal temporário podem ser uma fonte particular de vulnerabilidade, por isso, certifique-se de que recebem formação completa e adoptam as suas políticas de cibersegurança antes de trabalharem para si.

Segurança e gestão de dados

Os dados são a força vital de qualquer organização e incluem informações sobre o pessoal, os clientes, os parceiros, as suas redes e as actividades da organização. Manter

a segurança e a privacidade no que respeita a estes dados deve ser uma prioridade muito elevada. Para o efeito, recomendam-se as seguintes boas práticas.

- Faça cópias de segurança, vezes sem conta. Mantenha várias cópias seguras dos seus dados cruciais para que seja mais fácil recomeçar caso seja pirateado ou sujeito a um ataque de ransomware.
    - Decida se pretende fazer isto na Nuvem ou em vários discos rígidos seguros em diferentes locais (ou mesmo em papel).
        - Locais separados são importantes em caso de arrombamento, incêndio ou catástrofe natural
    - Considere a possibilidade de ter cópias de segurança em dispositivos com sistemas operativos diferentes (um em Windows e outro em macOS ou Linux) no caso de um sistema inteiro ser comprometido.
- Existem diversas opiniões sobre os prós e os contras de cada opção, dependendo em grande parte das suas prioridades e conhecimentos, mas o importante é certificar-se de que faz cópias de segurança dos dados.
- Conheça a situação legal no seu país no que respeita às suas práticas de gestão de dados e garanta o seu cumprimento.
    - O GDPR (Regulamento Geral sobre a Protecção de Dados) europeu é um modelo útil a seguir se ainda não tiver uma política nacional
- No mínimo, certifique-se de que tem autorização dos indivíduos para guardar quaisquer informações/dados pessoais sobre eles.
    - E apague todas essas informações que não precisar de as guardar.
        - Verifique regularmente com as pessoas sobre as quais tem informações se elas concordam que continue a tê-las.
- Certifique-se de que as informações privadas sobre as pessoas são sempre guardadas em ficheiros protegidos por palavra-passe e em pastas encriptadas.
    - E certifique-se de que mantém um registo seguro de todas as chaves/palavras-passe.
- Limite o acesso do pessoal a dados privados sobre outros funcionários e clientes (texto, imagens, áudio, vídeo) com base no princípio da necessidade de conhecimento.

Os sistemas digitais da sua organização

Os sistemas digitais de uma organização podem ser considerados como tendo três elementos interligados: dispositivos, software e redes.

Dispositivos

- Compre apenas hardware de fontes fiáveis.
- Reponha na fábrica todos os dispositivos em segunda mão.
- Certifique-se de que actualiza os sistemas operativos (geralmente Windows, macOS ou Linux) sempre que é lançada uma nova versão.
- Certifique-se de que todos os dispositivos estão fisicamente protegidos.
    - As invasões físicas são uma fonte comum de perda de dados e a substituição de hardware é dispendiosa.
    - Se o seu dispositivo móvel for roubado, certifique-se de que apaga todos os dados remotamente o mais rapidamente possível (utilizando a aplicação ‘’Encontrar o meu dispositivo’’ para Android ou a aplicação ‘’Encontrar meu

iphone'' para iPhones - lembre-se de ter estas aplicações activadas antes de perder o seu dispositivo)

- Não permita a utilização de cabos USB para transferência de dados entre dispositivos.
- Considere a utilização de um disjuntor para proteger o seu circuito elétrico dos danos causados por um circuito elétrico.
- Limite a sua utilização de dispositivos "inteligentes", pois, de um modo geral, todos eles podem ser utilizados para seguir a sua utilização e podem ser uma fonte de vulnerabilidades.

Software

- Utilize software antivírus de alta qualidade e analise os dispositivos regularmente.
  - Está disponível gratuitamente um bom software antivírus (bons exemplos incluem Avast, AVG, Avira, Bitdefender, McAfee, Norton e Sophos - a escolha depende um pouco do seu Sistema Operativo).
  - Certifique-se de que possui antivírus, protecção Web, ransomware e capacidades de retenção de tráfego malicioso.
  - Lembre-se de efetuar verificações completas de todos os dispositivos regularmente (de preferência, pelo menos, mensalmente).
  - Considere a possibilidade de subscrever uma fonte fiável que forneça informações sobre as mais recentes burlas e golpes (muitas vezes gratuitas), como
    - Experian https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware-of/
    - Ofcom (Reino Unido) https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/top-tips-to-stay-safe-from-scammers/
    - QUAL (WHICH) https://www.which.co.uk/news/article/the-latest-scam-alerts-from-which-aBRLy2b02WkC
- Compre apenas software de fontes ou fornecedores fiáveis.
  - Ou utilize software de código aberto (Open Source) fiável se estiver familiarizado com a forma de o instalar e utilizar.
  - Lembre-se de que existe muito software gratuito ou de baixo custo disponível.
  - Nunca utilize software pirata
    - Pode muito bem conter código malicioso.
    - É provável que esteja desatualizado e não contenha as últimas correcções de segurança.
- Certifique-se de que a maioria dos utilizadores da sua organização não tem "estatuto de administrador" ou "acesso" e tente limitar a utilização do software apenas àqueles que realmente precisam de o utilizar.
  - Adopte o princípio do privilégio mínimo, que limita as permissões desnecessárias de alto impacto (como o acesso de administrador) a acções potencialmente prejudiciais através de uma conta comprometida.
  - Monitore regularmente as contas de utilizadores administradores para garantir que não foram comprometidas.
- Actualize sempre o software assim que estiverem disponíveis novas versões.
  - Estas contêm normalmente actualizações de segurança que ajudam a proteger os seus sistemas.

- Tal como referido anteriormente, certifique-se de que todos os utilizadores possuem palavras-passe complexas.
- Limite as aplicações e o software disponíveis nos dispositivos da organização.
    - Não permita que as pessoas carreguem o seu próprio software nos dispositivos da organização.

Redes

- Utilize um fornecedor de Internet, um fornecedor de serviços na nuvem e um fornecedor de serviços geridos fiáveis
    - Assegure-se de que têm práticas claras de segurança desde a concepção.
    - Isto ajuda a limitar os potenciais riscos da cadeia de abastecimento.
- Certifique-se de que os seus routers e quaisquer dispositivos IoT (Internet of Things) estejam protegidos por palavra-passe com palavras-passe complexas que são alteradas regularmente.
- Crie uma rede para convidados no seu WiFi, caso pretenda fornecer acesso a convidados.
    - Isto permite-lhe ter a sua rede principal separada atrás de uma firewall que ajuda a protegê-la de ataques maliciosos.
- Não afixe as palavras-passe das suas redes WiFi de forma visível em paredes ou quadros de avisos onde possam ser facilmente fotografadas (nem que seja por acidente).
- Certifique-se de que todos os acessos externos aos seus sistemas passam por uma VPN (Rede Privada Virtual).

A sua página Web

A sua página Web é a sua janela para o mundo. Os conselhos que se seguem devem ajudá-lo a manter uma presença segura:

- Lembre-se de que tudo o que está na tua Web pode ser copiado e utilizado noutras páginas da Web.
    - O que é que não quer que as pessoas vejam?
- Certifique-se de que utiliza um fornecedor fiável e seguro para alojara sua página Web.
- Faça regularmente cópias de segurança dos dados da sua página Web.
- Tenha uma política clara sobre as imagens que pretende mostrar na sua página web e garanta o seu cumprimento. Pense especialmente em:
    - Caso pretenda mostrar o rosto das pessoas ou permitir a sua identificação.
        - Isto é especialmente importante se estiver a trabalhar com adultos e crianças potencialmente vulneráveis.
- Sempre que possível, obtenha um certificado SSL (Secure Sockets Layer) que lhe permite utilizar protocolos de transferência de hipertexto seguros (https) em vez de apenas http. Em https, o browser e o servidor estabelecem uma ligação segura e encriptada antes de transferirem dados.
- Teste frequentemente a sua página Web para detectar potenciais vulnerabilidades de segurança.
- Mantenha o nome de domínio/endereço (URL) tão curto, mas significativo, quanto possível.
- Em geral, evite ligações diretas a endereços de correio eletrónico para dificultar a sua recolha por programas automáticos.

    - Utilize uma página de contacto que direccione as mensagens para si.
        - Possivelmente também utilizando um CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
    - Ou utilize uma imagem do seu endereço de correio eletrónico.
    - Ou utilize o formato a(dot)person(at)organization(dot)org
- Algumas organizações preferem ter apenas um único endereço de correio eletrónico de ponto de contacto externo, como info@organisation.org.
- Actualize sempre os seus add-ons e plugins.
- Normalmente, é boa prática autorizar apenas um pequeno número de pessoas a criar e carregar material na tua Web.
    - Mantenha todos os nomes de utilizador e palavras-passe de acesso confidenciais.
    - Utilize diferentes níveis de segurança para diferentes tipos de utilizadores e tenha apenas uma ou duas contas de administrador.
- Siga as orientações ou restrições nacionais relativas as páginas Web.
    - Considere a possibilidade de ter políticas sobre a utilização de dados e cookies (ficheiros utilizados pelos servidores Web para guardar informações sobre os utilizadores) para explicar aos utilizadores como pode estar a utilizar os seus dados e dar-lhes opções relativamente a essa utilização.
- Não precisa de gastar muito na concepção de uma página Web dispendioso, mas tente mantê-lo simples e claro para transmitir as mensagens que pretende.
- Considere a possibilidade de efetuar testes de vulnerabilidade e penetração (VAPT), se tiver dinheiro para isso.

Redes sociais

A maioria das organizações da sociedade civil vai querer ter uma presença nas redes sociais para divulgar o seu trabalho e estabelecer contacto com os clientes, mas deve ter sempre cuidado com as inseguranças relacionadas com a utilização das redes sociais.

- Pense cuidadosamente nas plataformas de redes sociais que pretende utilizar, tendo em conta que todas elas lucram de alguma forma com os dados que extraem de si.
- Permita que apenas um número muito reduzido de pessoas com formação adequada e que conheçam bem a sua organização carreguem material para as suas contas nas redes sociais
- Utilize nomes de utilizador e palavras-passe complexos em todo o lado (ver comentários semelhantes acima).
- Restrinja a participação em grupos de redes sociais a pessoas de confiança.
    - Os grandes grupos do WhatsApp são particularmente vulneráveis porque podem ser utilizados para aceder a dados pessoais dos membros do grupo.
    - No Facebook, por exemplo, utilize regras de grupo e certifique-se de que as pessoas concordam com elas antes de lhes permitir a participação.
- Sempre que possível, utilize aplicações de mensagens encriptadas, como o Signal.
    - O WhatsApp também utiliza a encriptação de ponta a ponta do Signal em todas as mensagens.
    - Se utilizar o Telegram, mude sempre para o modo "Secret Chat" (Conversa secreta), mas mesmo assim a encriptação de ponta a ponta só é suportada para dois participantes.

- Não permita que ninguém (incluindo pessoal, clientes e visitantes) publique imagens das suas actividades ou do seu pessoal sem autorização expressa.

E-mails

Os e-mails são a fonte de muitas vulnerabilidades e os ataques a contas de e-mail estão a tornar-se cada vez mais comuns.

- Tenha um sistema que forneça regularmente a todo o pessoal lembretes sobre a segurança do correio eletrónico e notificações sobre novos tipos de ameaças ou burlas (ver acima) assim que tiver conhecimento delas.
- Parta do princípio de que qualquer mensagem de correio eletrónico recebida que não seja uma resposta a uma mensagem de correio eletrónico enviada pela sua organização pode ser uma ameaça.
- Nunca clique numa ligação numa mensagem de correio eletrónico, a menos que tenha a certeza de que é genuína e segura. Mesmo assim, pense duas vezes.
- Utilize filtros de SPAM definidos para um nível de protecção elevado (se possível).
- Utilize DMARC (*Domain Message Authentication Reporting* - Relatório de autenticação de mensagens de domínio)
- Incentive todo o pessoal a contactar a pessoa responsável pela segurança digital se suspeitarem de uma mensagem de correio eletrónico e, definitivamente, antes de a abrirem.
- Considere a possibilidade de definir regras para as mensagens de correio eletrónico recebidas que apenas permitam a aceitação de mensagens de correio eletrónico de contactos de confiança.
    - Isto pode ser muito eficaz quando utilizado em conjunto com as páginas de contacto (ver acima).
- Utilize sempre o bcc (cópia oculta) se enviar uma mensagem de correio eletrónico para muitas pessoas.
    - Para que não recebam todos os endereços de correio eletrónico uns dos outros.

Conclusões

Não é possível estar 100% seguro, mas seguir os conselhos acima referidos ajudá-lo-á a reduzir a probabilidade de a sua organização ser prejudicada por um incidente de cibersegurança. Alguns lembretes finais:

- **Considere provável que venha a ser afectado por um incidente de cibersegurança.**
- **Tenha um plano para atenuar o impacto de um ciberataque.**
- **Nomeie uma pessoa adequada para assumir a responsabilidade pela segurança digital como parte da sua portfolio.**
- **Dê regularmente formação a todo o seu pessoal (incluindo voluntários e pessoal temporário) sobre as suas práticas de cibersegurança.**
- **Utilize sempre palavras-passe complexas e autenticação multi-factor.**
- **Procure ajuda profissional o mais rápido possível se for alvo de um ataque cibernético.**

Anexo: Material que pode ser facilmente transformado em cartazes ou utilizado como panfleto em cursos de formação

De Hive Systems https://hivesystems.com/password
O tempo que um hacker demora a aplicar força bruta à sua palavra-passe em 2025. Os ataques de força bruta utilizam sistematicamente uma abordagem de tentativa e erro para identificar identidades de início de sessão, credenciais e chaves de encriptação. São utilizadas combinações de nomes de utilizador e palavras-passe até ser encontrada a combinação correcta. Os computadores são capazes de o fazer muito rapidamente e os computadores quânticos poderão, no futuro, reduzir drasticamente estes tempos. É essencial utilizar vários métodos de autenticação para ajudar a reduzir estas ameaças.

Time it takes a hacker to brute force your password in 2025

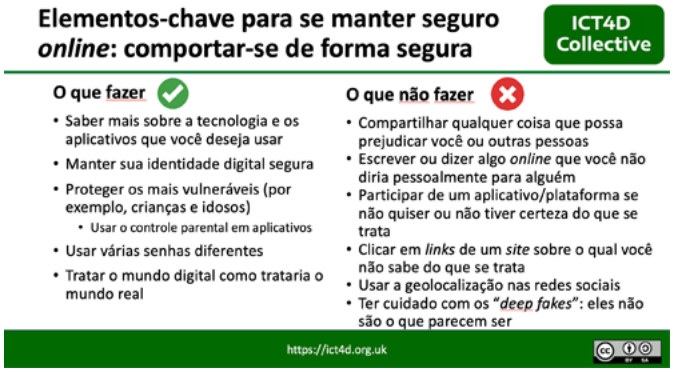
Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

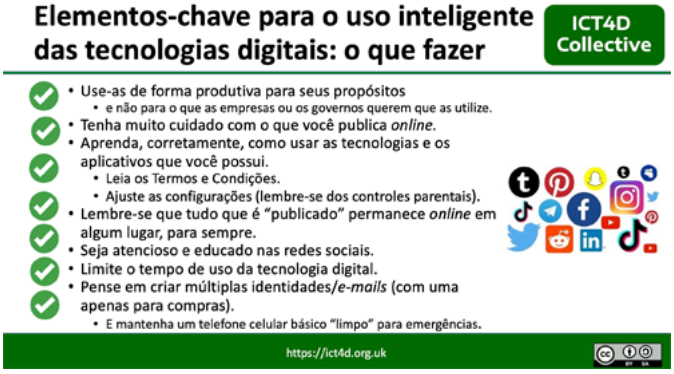
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at hivesystems.com/password

Do Coletivo ICT4D
Três exemplos dos diversos recursos desenvolvidos principalmente durante e após o nosso trabalho como parte do projeto MIDEQ financiado pelo UKRI GCRF (vide o nosso trabalho sobre migração e tecnologia digital). Estes materiais podem ser facilmente impressos e afixados nas paredes do escritório como simples lembretes. Os conjuntos completos de materiais sobre diferentes tópicos relacionados com a utilização segura, inteligente e protegida da tecnologia digital, com gráficos em várias línguas, estão disponíveis em https://ict4d.org.uk/sws/ .





Outros recursos

A maior parte deles são guias simples, fiáveis, curtos, claros e de fácil acesso sobre aspectos específicos da cibersegurança; alguns são guias mais longos, com mais pormenores, especificamente relacionados com as necessidades das organizações da sociedade civil.

Canadian Centre for Cyber Security (2024) Mitigating cyber threats with limited resources: guidance for civil society, https://www.cyber.gc.ca/en/news-events/mitigating-cyber-threats-with-limited-resources-guidance-civil-society.

CISA (Cybersecurity and Infrastructure Security Agency, EUA) (2024) *Mitigating cyber threats with limited resources: guidance for civil society*, https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf

Civicus (2022) Safety & cyber security: 8 tips for civil society digital defense, https://www.civicus.org/index.php/media-resources/news/blog/6118-safety-cyber-security-8-tips-for-civil-society-digital-defense .

Cloudflare (sem data) How to secure a website, https://www.cloudflare.com/en-gb/learning/security/how-to-secure-a-website/.

Coulson, G. (Betterteam) (2024) Cyber security policy overview and sample template, https://www.betterteam.com/cyber-security-policy.

Crowdstrike (2024) 12 tipos mais comuns de ciberataques, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.

GDPR.EU (2018) What is GDPR, the EU's new data protection law?, https://gdpr.eu/what-is-gdpr/.

Gov.UK (sem data) The National Cyber Security Centre, https://www.ncsc.gov.uk/.
IT Force (sem data) 5 políticas de cibersegurança de que todas as médias empresas necessitam, https://www.itforce.ca/blog/cybersecurity-policies-every-business-needs.
Instituto Nacional Democrático (2022) *Cybersecurity Handbook for Civil Society Organizations (Manual de Cibersegurança para Organizações da Sociedade Civil*), https://www.ndi.org/publications/cybersecurity-handbook-civil-society-organizations.
Rubenking, N.J. (2024) O melhor software antivírus gratuito para 2024, *PC Mag*, https://uk.pcmag.com/antivirus/120817/the-best-free-antivirus-protection.
Splunk (2023) Top 50 Cybersecurity Threats, https://www.splunk.com/en_us/form/top-50-security-threats.html.
Guia do Tom (2024) As melhores aplicações de mensagens encriptadas em 2024, https://www.tomsguide.com/reference/best-encrypted-messaging-apps.
Modelo de política de cibersegurança da empresa viável (2024), https://resources.workable.com/cyber-security-policy.

Autoria e agradecimentos

Versão 6: Este material foi inicialmente preparado por Tim Unwin em junho de 2024 em nome do ICT4D Collective, e foi subsequentemente revisto em julho de 2024, com agradecimentos especiais aos comentários de G. "Hari" Harindranath, Jamie Proctor e Jamie Saunders. Foram feitas novas revisões em agosto de 2024, com agradecimentos a Danilo Pereira Sato, e actualizado em maio de 2025 para incluir ameaças mais recentes. Esta tradução foi feita por Eliseu Silvestre Canuma.