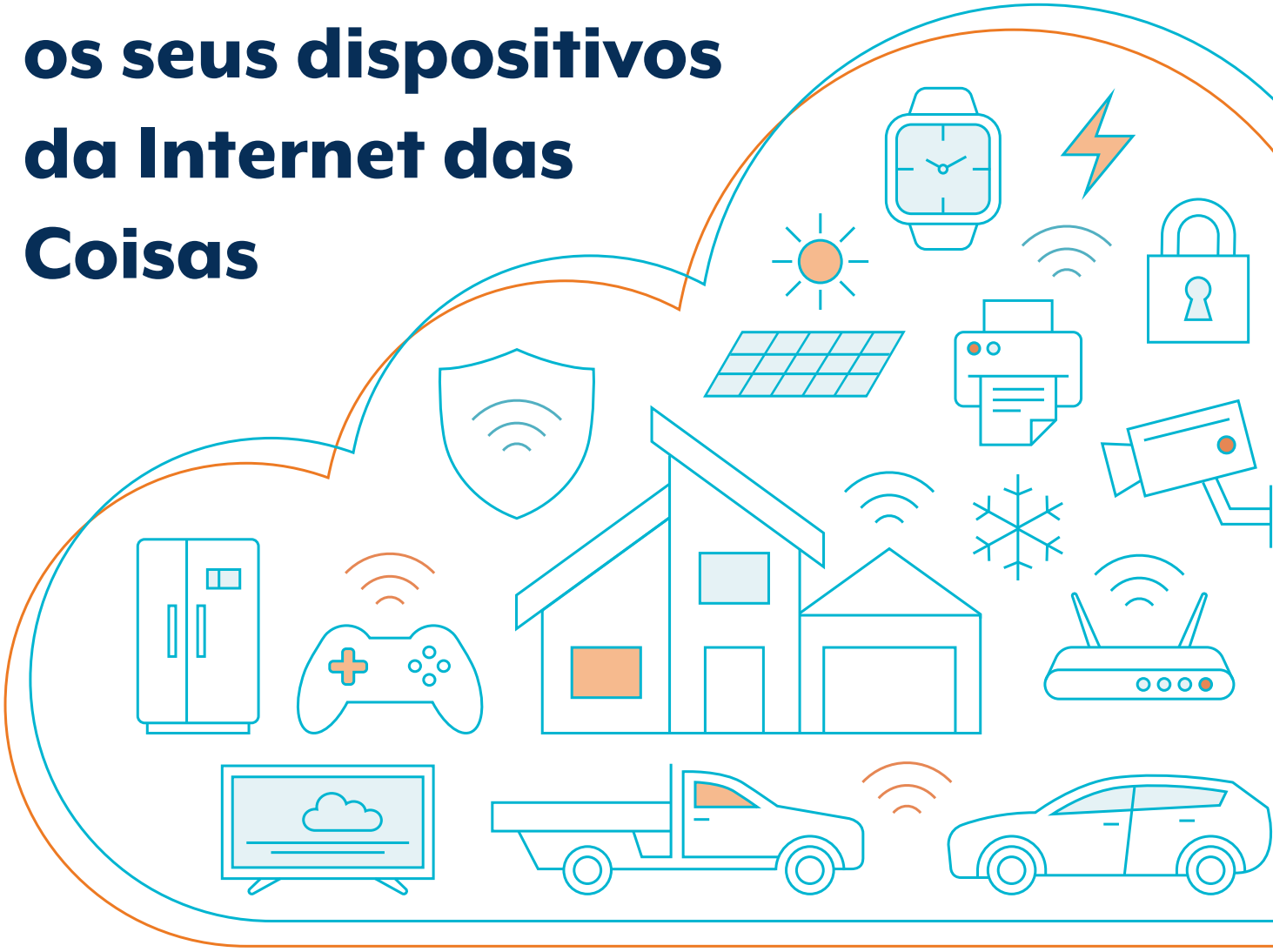
Dicas para proteger os seus dispositivos da Internet das Coisas



O Centro Australiano de Segurança Cibernética desenvolveu esta informação para ajudar a comunidade a comprar e utilizar os dispositivos da Internet das Coisas (IoT) de forma segura. Um dispositivo IoT é um objecto do dia-a-dia ao qual foi adicionada conectividade de internet. Exemplos de dispositivos IoT incluem monitores de bebé, drones, câmeras de vigilância, televisões inteligentes e inversores solares. Os dispositivos IoT nas residências e empresas geralmente usam redes WiFi ou celulares como 4G ou 5G para se ligar à intenet.

Muitos dispositivos IoT normalmente encontrados nas residências e empresas australianas não foram concebidos visando a segurança. Isto resultou em dispositivos vulneráveis a serem comprometidos através da internet. Tais incidentes podem permitir que os cibercriminosos tenham acesso não solicitado ao seu dispositivo e dados pessoais para fins maliciosos.

Antes de comprar um dispositivo IoT

É importante pesquisar dispositivos antes de fazer uma compra, porque os fabricantes oferecem vários níveis de segurança. Antes de comprar um dispositivo, compare dispositivos semelhantes vendidos por diferentes fabricantes. As coisas que deve considerar incluem:

1. **O dispositivo foi fabricado por uma empresa conceituada e respeitável e vendida numa loja de renome e boa reputação?** As empresas de renome e boa reputação são mais propensas a produzir dispositivos que focam na segurança. As lojas de renome e boa reputação são mais propensas a vender apenas dispositivos de empresas de renome e boa reputação e têm uma cadeia de suprimento mais rigorosa que assegura que o dispositivo chegue às suas mãos conforme a intenção do fabricante.

2. **É possível mudar a palavra-passe?** É sempre bom mudar a sua palavra-passe. No entanto, se o dispositivo for expedido com uma palavra-passe padrão fraca, isso torna-se mais importante. Um dispositivo com boa segurança deve ter uma palavra-passe única, imprevisível, complexa e improvável de adivinhar, porque as palavras-passe padrão fracas são a maneira mais fácil de atacar um dispositivo.

3. **O fabricante fornece atualizações?** É importante que as empresas ofereçam atualizações para resolver as vulnerabilidades do dispositivo à medida que forem descobertas. Por exemplo, se o software do dispositivo contiver vulnerabilidades conhecidas ou os hackers desenvolverem novas maneiras de comprometer o seu dispositivo, são necessárias atualizações para fornecer correções.

4. **Que dados o dispositivo recolherá e com quem esses dados serão partilhados?** A informação sobre os dados que o dispositivo irá recolher e como eles serão utilizados deverá estar prontamente disponível no site do fabricante ou na sua política de privacidade. É importante ter sempre em consideração a informação que a aplicação online ou móvel recolhe.

5. **O dispositivo faz apenas aquilo que você quer que ele faça?** Comprar um dispositivo que faz mais do que aquilo que você precisa, incluindo ligação à internet, poderá reduzir a sua segurança. Os recursos de dispositivo que você não usará podem aumentar a vulnerabilidade do dispositivo contra ataques, sem quaisquer benefícios para si.

Dispositivo IoT

Lembre-se de algumas perguntas simples quando configurar o seu dispositivo, para ajudá-lo a manter a sua rede e os seus dados mais seguros.

1. **O seu dispositivo precisa de ser ligado à internet?** Só pelo facto de poder ser ligado não significa que deve ser ligado. Os dispositivos que não estão ligados à internet têm uma probabilidade muito menor de serem comprometidos. Se vai utilizar os recursos que necessitam ligação à internet, deve considerar se precisa ou não de estar ligado.

2. **O dispositivo está num local seguro?** Se o dispositivo não precisa de ser instalado numa área não segura, instalá-lo num local seguro poderá reduzir o risco de comprometimento físico.

3. **Devo mudar o nome de utilizador e a palavra-passe padrão?** É importante que você utilize uma palavra-passe ou frase-passe fortes. Se o seu dispositivo não for expedido com uma palavra-passe única, imprevisível, complexa e improvável de adivinhar, essa palavra-passe precisa de ser mudada. Os nomes de utilizador e palavras-passe predefinidos são recolhidos e publicados online, tornando o seu dispositivo vulnerável.

4. **Aminha rede Wi-Fi está configurada com segurança, e tem uma palavra-passe segura?** Proteja sua rede Wi-Fi e roteador para dificultar o acesso de atacantes ao seu dispositivo e à sua rede.

Vá mais além

Instale uma rede Wi-Fi adicional no seu roteador somente para dispositivos IoT. Esta pode ser conhecida no seu roteador de Wi-Fi como uma rede de 'convidados'. Se os seus dispositivos IoT não precisam de comunicar entre eles, desative o recurso 'isolamento do cliente'. Manter os seus dispositivos IoT isolados dos seus dados confidenciais assegura que um comprometimento de um dispositivo IoT não permite acesso aos seus outros dispositivos ou dados.

5. **Os recursos desnecessários do dispositivo estão desativados?** Se o seu dispositivo tiver recursos indesejados ou desnecessários (tais como câmeras ou microfones), estes devem ser desativados quando possível.

Vá mais além

Procure uma configuração que mencione a ativação de acesso remoto à interface de administração web do dispositivo a partir da LAN local ou WAN/internet. Assegure-se que ele está definido para LAN local, salvo você próprio precise de acesso remoto.

Manutenção de um dispositivo IoT

Há algumas coisas importantes para lembrar assim que o seu dispositivo IoT estiver configurado e em uso. Estas incluem:

1. **Reiniciar os seus dispositivos regularmente.** Podem estar presente vírus se o seu dispositivo IoT começar a ficar lento ou inoperante. A maioria do malware é armazenado na memória e pode ser removido facilmente por uma reinicialização do dispositivo, isto é, desligando e ligando novamente o dispositivo. Se o dispositivo continuar a ser lento e inoperante depois da reinicialização, tente uma redefinição de fábrica, no entanto esteja ciente que isto poderá apagar todos os seus dados de utilizador e configurações personalizadas.

2. **Aplicar atualizações regulares.** Alguns dispositivos aplicam atualizações automaticamente. Para aqueles que não o fazem, verifique regularmente junto ao fabricante e aplique as atualizações quando estiverem disponíveis. Quando as atualizações já não estiverem disponíveis para o seu dispositivo, pense em atualizar para um dispositivo mais novo que tenha atualizações disponíveis. Dispositivos que não têm acesso a atualizações de segurança não serão protegidos se forem descobertas novas vulnerabilidades, e esses dispositivos poderão tornar-se um risco para a sua rede, sua privacidade e seus dados.

3. **Desligue o seu dispositivo quando não estiver a ser utilizado.** Deixar dispositivos não utilizados e não monitorizados alimentados e ligados à sua rede Wi-Fi por longos períodos pode aumentar a probabilidade de os seus dispositivos serem atacados. Uma opção para conseguir isto automaticamente é utilizar um temporizador de tomada para fornecer energia ao dispositivo somente durante um período específico.

4. **Esteja atento a um aumento significativo no seu uso mensal de internet ou na sua conta.** Aumentos significativos no uso de Internet ou nas faturas podem indicar que o seu dispositivo está comprometido. A menos que isto seja investigado por um departamento de TI da sua empresa, deve ser aplicada uma redefinição de fábrica (no entanto, esteja ciente de que isto poderá apagar todos os seus dados de utilizador e configurações pessoais), seguida de uma mudança de palavra-passe.

Descartar um dispositivo IoT

Descartar um dispositivo (eliminando-o ou vendendo-o) pode dar acesso a outras pessoas à sua informação ou dados pessoais. As formas de evitar isto incluem:

1. **Apague todos os dados e informação pessoal.** O fabricante deve fornecer um método de como apagar os seus dados e informação pessoal tanto do dispositivo quanto das aplicações associadas. Apagar a sua informação pessoal assegura que ninguém tenha acesso a ela depois de você ter descartado o dispositivo. Elimine a sua conta online se já não precisar dela sem o dispositivo IoT.

2. **Efetue uma reposição de fábrica do dispositivo.** Uma reposição de fábrica destina-se a apagar os dados armazenados localmente e redefinir palavras-passe, nomes de utilizadores e configurações de volta aos padrões. Consulte o manual de utilizador do dispositivo ou o site do fabricante para informação sobre como efetuar uma reposição de fábrica.

3. **Desassocie o dispositivo dos telemóveis e outros dispositivos.** Descartar um dispositivo que ainda tem acesso aos seus outros dispositivos, rede ou contas online tem potencial para que outros tenham acesso. Assegure-se que verifica os seus outros dispositivos e remove qualquer pareamento com o dispositivo que está a descartar. Remova quaisquer permissões concedidas à aplicação móvel que já não necessita.

4. **Remova qualquer mídia removível (ex. pen drives cartões de memória etc.) ligada ao dispositivo.** A mídia removível pode conter dados pessoais que não são apagados numa reposição de fábrica e deve ser fisicamente removida, destruída e descartada separadamente do dispositivo.

Ajuda

Contacte o Centro Australiano de Segurança Cibernética da Direção Australiana de Sinais enviando e-mail para asd.assist@defence.gov.au ou ligue para a linha direta 24 horas por dia, 7 dias por semana, para assistência urgente no **1300 CYBER1** (**1300 292 371**).

Denuncie um crime cibernético a ReportCyber no www.cyber.gov.au/report

Contacte IDCARE através do seu site www.idcare.org se foi vítima de roubo de identidade.

Visite www.cyber.gov.au para aconselhamento para si e a sua família. Inscreva-se gratuitamente para o Serviço de Alerta ACSC sobre ameaças online recentes.

Vamos tornar a Austrália o lugar mais seguro para ligação online.

Para conselhos sobre a segurança cibernética, visite www.cyber.gov.au

Isenção de responsabilidade

O conteúdo deste guia é de natureza geral e não deve ser considerado como aconselhamento jurídico, nem utilizado como referência em circunstâncias específicas ou situações de emergência. Em qualquer assunto importante, deve procurar o aconselhamento profissional independente adequado em relação às suas circunstâncias pessoais.

A Commonwealth não se responsabiliza por quaisquer danos, perdas ou despesas incorridos como resultado da confiança nas informações contidas neste guia.

Para mais informação ou para denunciar um incidente de segurança cibernética, contacte-nos:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Este número está disponível para uso apenas dentro da Austrália.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre