CIBERSEGURANÇA — GUIA PRÁTICO

Garanta a Segurança do Seu Router e do Wi-Fi: O Que Precisa de Saber Sobre o SSID

O router é a porta de entrada da sua rede. Quem o controla, controla tudo o que passa por ele — conversas, pagamentos, passwords. Este guia mostra-lhe como fechar essa porta a intrusos.

A maioria das pessoas bloqueia a porta de casa, mas deixa a rede Wi-Fi praticamente aberta. Um atacante não precisa de estar fisicamente presente para aceder ao seu router — basta estar no estacionamento da sua rua.

1. O Que É o SSID e Porque É Importante

O SSID (Service Set Identifier) é, simplesmente, o nome da sua rede Wi-Fi. É aquilo que vê quando pesquisa redes disponíveis no seu telemóvel: "MEO-CASA", "NOS_2.4G", "VODAFONE-ABCD", ou na maioria das casas o nome que veio de fábrica.

O problema começa precisamente aqui. O nome padrão do fabricante anuncia ao mundo o modelo exato do seu router. E um atacante que conheça o modelo, conhece também as vulnerabilidades conhecidas desse equipamento.

Exemplos de SSID — o que revelar e o que evitar

`ZTE_ZXHN_H208N_ABCD`	**Revela fabricante e modelo**
`MEO-45A2`	**Identifica o operador**
`Casa dos Silva`	**Identifica o proprietário**
`Armazem_Loja_2024`	**Identifica negócio e ano**
`Rede-7F3K`	**Neutro — não revela nada**
`WifiVisitantes_Cafe`	**Aceitável (rede separada)**

2. Os Perigos Reais: O Que Pode Correr Mal

Estes não são cenários hipotéticos. São ataques documentados que acontecem em habitações, pequenas empresas e espaços comerciais todos os dias.

Exemplos de ataques mais comuns:

ATAQUE 1

Acesso à rede local

O atacante liga-se à rede e passa a ver todos os dispositivos: câmeras, impressoras, NAS, computadores. Pode copiar ficheiros, instalar malware ou espiar o tráfego.

ATAQUE 2

Roubo de credenciais

Através de um ataque man-in-the-middle, o atacante intercepta logins de homebanking, e-mail e redes sociais sem que o utilizador dê conta.

ATAQUE 3

Router como proxy ilegal

A sua ligação à internet é usada para actividades ilegais — descarregar conteúdos piratas, lançar ataques a terceiros. A responsabilidade legal pode recair sobre si.

ATAQUE 4

DNS Hijacking

O atacante altera as configurações de DNS do router. Quando escreve um endereço de banco, é redirecionado para uma cópia falsa do site que rouba as suas credenciais.

ATAQUE 5

Evil Twin (Gémeo Malicioso)

É criada uma rede com o mesmo nome do seu SSID. Os dispositivos ligam-se automaticamente ao sinal mais forte — que é o do atacante.

ATAQUE 6

Exploit de firmware

Routers com firmware desatualizado têm vulnerabilidades conhecidas e publicadas online. Um script automatizado pode comprometer o seu router em segundos.

RISCO CRÍTICO

Em 2023, o CERT-PT registou um aumento de 340% em ataques a dispositivos domésticos.

A maioria explorou passwords padrão e firmware desatualizado — problemas que se resolvem em 10 minutos.

3. Vulnerabilidades Mais Comuns — Por Ordem de Risco

Password padrão do router Crítico

"admin/admin", "admin/password", "1234" — são as primeiras combinações que qualquer atacante testa. O manual do utilizador do seu router (facilmente encontrado online com o número de modelo) lista as credenciais padrão.

Protocolo WEP ou WPA (versão 1) Crítico

O WEP foi quebrado em 2001. O WPA em 2008. Usar qualquer um destes é o equivalente a ter uma fechadura de plástico na porta de casa. Use apenas WPA2 ou WPA3.

Firmware desatualizado Alto

Fabricantes lançam atualizações que corrigem vulnerabilidades de segurança. Um router sem atualizações há 2 anos tem, provavelmente, dezenas de falhas conhecidas e não corrigidas.

WPS ativado Alto

O botão WPS (para ligar dispositivos facilmente) tem uma vulnerabilidade que permite quebrar a password da rede em poucas horas com ferramentas gratuitas. Desative-o.

Gestão remota ativada Médio
Se a interface de configuração do router está acessível a partir da internet, qualquer pessoa no mundo pode tentar entrar. Na grande maioria dos casos, deve estar desativada.

SSID visível com nome revelador Médio
Revela o fabricante, o modelo ou a identidade do proprietário, facilitando ataques dirigidos.

4. Como Aceder às Configurações do Router

Antes de fazer qualquer alteração, precisa de entrar no painel de administração do router. Não é complicado — é como aceder a um site.

COMO ENTRAR
1. Abra um browser (Chrome, Edge, Firefox) num dispositivo ligado à sua rede.
2. Escreva na barra de endereço: 192.168.1.1 ou 192.168.0.1 (tente os dois).
3. Surgirá uma página de login. Use as credenciais — se nunca as alterou, estão na etiqueta colada na parte de baixo do router.
4. Após entrar, nunca mais saia sem alterar a password de acesso ao painel.

5. Lista de Ações: O Que Fazer Agora

Organize estas tarefas por ordem. As primeiras são as mais urgentes.

1. **Altere imediatamente a password de administração do router.** Use uma combinação de letras maiúsculas, minúsculas, números e símbolos, com pelo menos 12 caracteres. Nunca use datas de nascimento ou nomes.
2. **Mude o nome do SSID** para algo neutro que não revele o fabricante, o modelo, o seu nome ou o nome do negócio. Evite também usar o ano — denuncia que a rede não é atualizada.
3. **Defina a password do Wi-Fi com WPA2 ou WPA3.** Use uma frase-chave longa e fácil de lembrar, mas difícil de adivinhar: por exemplo, "CafedoJoao#Alfama2!" é muito mais segura do que "Joao2021".
4. **Atualize o firmware do router.** No painel de administração, procure "Atualização de firmware" ou "Firmware Update". Se o seu router já não recebe atualizações há vários anos, considere substituí-lo.
5. **Desative o WPS.** No painel do router, procure "WPS" e desative a opção. Se não encontrar, consulte o manual do modelo específico.
6. **Desative a gestão remota** (Remote Management / Remote Access). Só deve ativar se souber exatamente o que está a fazer e porquê.
7. **Crie uma rede de convidados separada** para visitas, clientes e dispositivos IoT (televisões, câmeras, termostatos). Estes dispositivos não devem ter acesso à sua rede principal.
8. **Verifique quem está ligado à sua rede.** No painel do router, procure "Dispositivos ligados" ou "DHCP Clients". Se vir algo desconhecido, investigue.

DICA PROFISSIONAL

Defina um lembrete recorrente — a cada 6 meses — para verificar se há atualizações de firmware e rever quem está ligado à rede.

A segurança não é um estado, é um processo contínuo.

6. Conselhos por Tipo de Espaço

As necessidades variam consoante o contexto. Aqui estão as prioridades específicas para cada situação.

HABITAÇÃO

Casa / Apartamento

- Uma rede principal + uma rede de convidados
- Dispositivos IoT na rede de convidados
- Password Wi-Fi partilhada apenas com residentes
- Mudar a password quando alguém sai de casa
- Router posicionado centralmente, não junto a janelas

TRABALHO

Pequena Empresa

- Rede separada para colaboradores e clientes
- Nunca partilhar a password de trabalho com visitas
- Registar quem tem acesso e revogar quando saem
- Considerar router com funções de segurança empresariais
- Garantir que o router está num local físico fechado

COMÉRCIO

Espaço Comercial

- Rede pública isolada da rede de gestão e PDQ
- Nunca processar pagamentos na mesma rede do Wi-Fi público
- Limite de velocidade na rede de clientes
- Monitorizar ligações suspeitas regularmente
- Mudar a password da rede pública mensalmente

ATENÇÃO — ESPAÇOS COMERCIAIS

Se aceita pagamentos com cartão, está sujeito à norma PCI DSS.

Esta exige que a rede que processa pagamentos esteja completamente isolada de qualquer rede pública de Wi-Fi.

A violação desta norma pode resultar em multas significativas e perda da capacidade de aceitar cartões.

A Última Linha de Defesa é o Conhecimento

Um atacante sofisticado escolhe sempre o alvo mais fácil. Um router bem configurado não é invulnerável — mas é suficientemente difícil de comprometer para que o atacante passe ao vizinho.

As medidas descritas neste guia não requerem conhecimentos técnicos avançados. Requerem apenas uma hora da sua atenção e a consciência de que a segurança digital começa em casa — ou mais precisamente, na caixa com luzes intermitentes que está algures na sua sala.

Se tiver dúvidas na implementação de qualquer um destes passos, contacte um técnico de informática ou o suporte do seu operador. A maioria das operadoras portuguesas oferece assistência remota gratuita para configurações básicas de segurança.