



Segurança e uso da Internet

Segurança no uso da Internet

Protecção da sua rede domestica wi-fi:

Uma rede wifi não protegida constitui uma grave falha de segurança, pois além permitir o uso indevido do seu serviço de internet por terceiros que estão na sua vizinhança levando a ter consumos de dados de Internet mensal acima do habitual e consequentemente, a uma facturação elevada do serviço, pode também comprometer a protecção dos seus dados pessoais e das informações que estão no seu computador.

Para proteger a sua rede doméstica de wifi, de utilização não autorizada por parte de terceiros que poderá estar na sua vizinhança, existem protocolos de segurança que permitem encriptar a sua conta através da utilização de palavra-passe. Normalmente os operadores disponibilizam essa palavra-passe no momento da instalação do serviço.

Dicas básicas para protecção da sua rede:

- Não divulgue a sua palavra-passe a terceiros;
- Altere a palavra-passe da sua rede wifi com alguma frequência;
- Não utilize palavras-passe demasiado fáceis de serem descobertos como 1234, o nome pessoal, dos filhos ou datas de nascimentos, números de telefone, entre outros;
- Utilize sempre caracteres especiais e uma mistura de letras e números na sua palavra-passe;
- É conveniente desligar sempre o router quando não estiver utilizando o serviço;
- Não identifique a sua rede wifi com o seu nome pois permitirá as pessoas detectarem facilmente a sua rede.

Como preservar o endereço de e-mail

Dicas para preservar o seu endereço de e-mail de mensagens Spam:

- Cuide de seu e-mail como cuida do endereço da sua casa. Não convém dar o endereço a qualquer estranho, nem mesmo fornecer esses dados sem perguntar o fim para qual lhe é solicitado. Logo, o seu e-mail deve ser tratado da mesma forma, para que não seja vítima de e-mails não solicitados.
- Utilize e-mails separados para uso pessoal, trabalho, compras on-line e cadastros em sites em geral. Assim, é possível mantê-los com caráter de "público", enquanto outros, são mantidos "restritos" ao trabalho e à família.
- Leia com atenção os formulários e cadastros on-line, evitando preencher ou concordar, inadvertidamente, com as opções para recebimento de e-mails de divulgação do site e de seus parceiros.
- Verifique a existência da política de privacidade dos sites, espaço para preenchimento de cadastros e formulários. A empresa que mantém o site, ao possuir uma política de privacidade, pode garantir que seus e-mails não serão repassados ou vendidos a terceiros.
- Evite utilizar e-mails simples e comuns (João, Maria, compras), pois podem ser facilmente descobertos por ferramentas automáticas ou por ataques de dicionário. O spammer forma endereços de e-mail a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.
- Evite colocar em sites os e-mails no formato comumente utilizado (fulano@dominio.cv), pois facilita a atuação bem-sucedida de ferramentas automáticas de harvesting (colheita) de e-mails. É recomendado, se necessário, implementar o contacto via formulário que não exiba o e-mail ou por meio de imagens.