Numa navegação livre na internet a segurança é o mais importante

Protecção cautelosa dos dados pessoais

Utilização inteligente da internet

Dicas de autoprotecção respeitantes à segurança na internet

Gabinete para a Protecção de Dados Pessoais

Endereço : Avenida da Praia Grande, n.º 804, Edif. China Plaza, 13.º Andar, A-F, Macau

Telefone : 2871 6006

Fax : 2871 6116

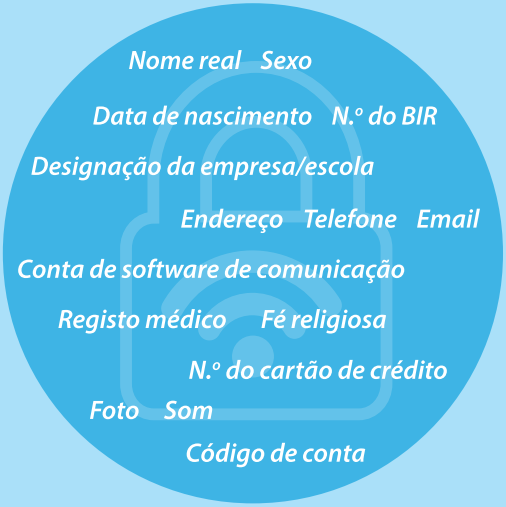
Email : info@gpdp.gov.mo

Endereço electrónico : www.gpdp.gov.mo

À medida que se desenvolvem as tecnologias da informação, a internet torna-se numa parte cada vez mais importante da nossa vida e quer a pesquisa online para obter informações, quer a aprendizagem online, as compras online, ou os contactos sociais, são facilidades e coisas agradáveis que a internet nos traz. No entanto, o mundo da internet é vasto e profundo, você sabe quantas armadilhas ocultas existem, de que resultam fugas de dados pessoais?

Dados pessoais

Em geral, dizemos que qualquer informação, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável é parte da privacidade pessoal. Por exemplo:



Eventuais consequências da revelação de dados pessoais na internet

- Os dados ficam conservados permanentemente na internet e podem ser pesquisados e divulgados por qualquer pessoa;
- A invasão por *hacker* ou a infecção do sistema por vírus facilita o furto de dados pessoais;
- O furto de identidade provoca prejuízos dos direitos e interesses;
- A revelação de dados pessoais permite o assédio cibernético ou os motores de pesquisa de carne e osso.

Cinco métodos de autoprotecção

1 Não publique indiscriminadamente dados pessoais ou familiares;

2 Pense bem antes de enviar mensagens;

3 Fique sempre alerta, não despreze a importância dos dados pessoais;

4 Tome medidas de segurança eficientes (instalação de *software antivirus* / *Firewall*) para diminuir o risco de intrusão por *hackers*;

5 Leia com cuidado a política de privacidade para tomar conhecimento da maneira de tratamento dos dados pessoais.

Sobre as redes sociais

As redes sociais fornecem-nos um instrumento que facilita a comunicação e interacção das pessoas. No entanto, as mensagens enviadas são difíceis de retirar definitivamente da internet, mesmo que sejam canceladas ou retiradas de imediato, pois ficam, na rede, registos que podem ser pesquisados e transferidos. Além disso, o excesso de partilha de dados pessoais próprios ou dos amigos pode causar prejuízos a si próprio ou a outras pessoas.

Armadilhas para a privacidade

1

"Visitar locais" na rede social pode revelar o seu paradeiro;

2

Mesmo dados fragmentários deixados em diferentes redes podem ser consolidados por vários canais;

3

Share

Clicar indiscriminadamente em "partilhar" ou "gosto" pode revelar os dados pessoais como endereço de email ou preferências pessoais a uma terceira pessoa;

4

Carregar fotos na rede pode revelar, inadvertidamente, dados que não são destinados à partilha.

Dicas de autoprotecção

Deve evitar fornecer demasiados dados pessoais na altura de criar uma conta nova;

Apenas permita a pessoas autorizadas ler os seus ficheiros e dados pessoais;

É preciso rever frequentemente a política actualizada da privacidade das redes às quais se liga, para saber quais são os dados partilhados.

O que não deve fazer

- Nas salas de *chat* online e nos diálogos directos, evite enviar dados pessoais importantes, como código, endereço, n.º de telefone etc. a fim de diminuir as possibilidades de fuga de dados;
- Não carregue fotos ou mensagens indiscriminadamente;
- Não publique arbitrariamente fotos ou dados de outrem. É preciso pedir consentimento ao interessado antes de compartilhar esses dados.

Sobre compras na internet

Hoje em dia está na moda fazer compras na internet, as várias modalidades de compras e pagamento facilitam os entusiastas da internet, mas envolvem também o tratamento de dados pessoais, e caso não tome cuidado, podem causar prejuízos tanto para o seu património como para a privacidade.

Armadilhas para a privacidade

É fácil permitir a fuga de dados da conta e do cartão de crédito, quando realiza transações em computadores públicos, telemóveis e plataformas de transação sem segurança;

As redes coleccionam as preferências dos consumidores através de *cookie*.

Dicas de autoprotecção

1

Faça compras online no seu computador pessoal que tenha instalado *software antivirus / Firewall*;

2

Frequente *hot sites* merecedores de confiança ou utilizados por amigos;

3

Tenha cuidado com o tratamento do n.º da conta e do código; use apenas plataformas de pagamento com tecnologia de encriptação para enviar dados como cartão de crédito.

Sobre navegação na internet/descarregamento de *software*

Tanto no computador, como no telemóvel, quando navega na internet, se regista na rede, descarrega *software*, participa em jogos ou em sorteios, primeiro tem que se inscrever, mas deve estar alerta para evitar fornecer demasiados dados.

Armadilhas para a privacidade

- Exigências de fornecimento de dados pessoais durante a promoção de jogos online ou na fase de progressão de nível;
- A ligação WI-FI sem segurança é como abrir a porta para deixar os ladrões entrar;
- Algumas aplicações são *software* malicioso, exigem uma grande quantidade de dados desnecessários para prestar funções simples;
- A utilização gratuita de um programa através de *"jailbreak"* provoca facilmente lacunas de segurança, deixando os vírus e aplicações maliciosas invadir e roubar dados de privacidade.

Dicas de autoprotecção

1. Utilização de uma conta de email específica para se registar na rede e receber email, pois quando tencionar cessar a comunicação com a rede, pode cancelar a conta;
2. *Download software* só na rede oficial;
3. Antes de submeter dados pessoais, deve ter bem claro a quem vai oferecê-los e se os dados pedidos são necessários e adequados;
4. Não clique em emails de origem desconhecida nem em hiperlinks nesses emails.

Conhecimentos

Cookie

Cookie é ficheiro de computador que regista a navegação dos utilizadores na internet, incluindo as preferências pessoais, as escolhas de carrinho de compras na rede e o histórico da navegação. O utilizador deve ter conhecimentos básicos sobre *cookie* para saber aceitá-lo e recusá-lo.

Senha (*Password*)

A senha deve ser composta por letras, algarismos e sinais de pontuação, evitando utilizar dados fáceis de adivinhar como 12345, a data de nascimento e o n.º de telefone etc.. Não utilize a mesma senha nas várias contas e renove-a frequentemente.

HTTPS

HTTPS (*Hypertext Transfer Protocol Secure* - protocolo de transferência de hipertexto seguro), quando o endereço de um sítio começa por https e tem o símbolo de uma fechadura, a ligação é encriptada satisfazendo requisitos essenciais de segurança e sendo mais segura do que a ligação a um sítio com endereço que começa por http.

Partilha de casos

Revelação do paradeiro pela partilha de fotos na internet

1. Uma pessoa chata costuma procurar, nas redes sociais, pessoa que acabou de carregar fotografias e que revelou o seu paradeiro por causa de "Visitar locais", tomando conhecimento da vida dele através das fotos carregadas e da renovação de estado, a seguir, dá mensagens a aquela pessoa, contando os assuntos acontecidos na vida dele para pregar-lhe um susto. Quando a técnica acima referida é utilizada pelos vilões, ninguém sabe o que vai acontecer.

2. Um homem criminoso da Inglaterra fugiu no período da fiança judicial. A polícia descobriu que ele se escondia na Espanha através de uma foto, com paisagem do pôr-do-sol numa galeria de palmeiras, carregada pelo criminal numa rede social. No fim, a parte da Inglaterra prendeu o criminal em colaboração com a polícia da Espanha, extraditou-o e condenou-o à prisão.

Perda de dinheiro por causa de descuido nas compras online

Um estudante de Macau fez compras online numa plataforma de pagamento e suspeitou que caísse num conto do vigário, o vigarista acedeu dados pessoais do estudante, através de um *site* de *phishing*, incluindo nome, conta bancária, n.º de telefone etc.. Posteriormente, o vigarista levantou, da conta de pagamento do estudante, cerca de dez mil patacas.

A extorsão tem origem na revelação dos próprios dados pessoais

Um jovem de Macau conheceu, através de uma aplicação de conhecer amigos novos, uma "rapariga", esta última propôs realizar transacção imoral, em contrapartida, o jovem recompensou-lhe com pontos de jogada. O jovem concordou e enviou-a o número do cartão de pontos de jogada, com valor mais de mil patacas, e a sua senha, a "rapariga" pediu-o ainda dados do BIR como garantia. Posteriormente, o jovem atendeu um telefonema de extorsão de um homem que falou mandarim, o qual intimidou o jovem que era desfavorável para os familiares dele se chamar a polícia, pois tinha dados pessoais do jovem.