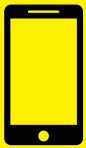
SERÁ QUE SABES TUDO SOBRE SMARTPHONES ?

O FABULOSO MUNDO DOS SMARTPHONES

Os telemóveis tornaram-se num equipamento essencial no dia-a-dia, tendo a sua evolução mais recente, os smartphones, chegado a um desenvolvimento tecnológico próximo de um computador pessoal e as atividades que necessitavam de aparelho ligado a um fio agora podem ser feitas "on the go". Um smartphone está equipado com software que permite a utilização de leitores de música e vídeo, navegador de internet, serviços de chat, chamadas pela Internet e vídeo-chamadas em tempo real, aplicações do estilo "office", georreferenciação, ligação às redes sociais e quase todas as atividades suportadas por um conjunto de aplicações (tanto pagas como gratuitas) que todos os dias são lançadas para os mercados.

O aumento do número de serviços disponíveis num Smartphone tem sido exponencial e espera-se que estes continuem a aumentar, fazendo com que as trocas de informação nas sociedades contemporâneas sejam cada vez mais mediadas por estes aparelhos. Não obstante existirem vários sistemas operativos (IOS, Android, Blackberry, Symbian, Windows Phone, etc), todos os smartphones funcionam de forma semelhante e oferecem os mesmos tipos de serviços.



O QUE PODE CORRER MAL COM UM SMARTPHONE?

Um smartphone, tal como os computadores, é vulnerável a certos perigos, como os do Phishing, SPAM, Malware, roubo de informação pessoal e/ou de identidade e também cyberbullying. Assim, a maioria das regras de segurança que se aplicam para os primeiros aplicam-se aqui também.

Tal como no computador, quando um smartphone fica infetado é possível detetar uma diminuição na sua performance, o aparecimento de aplicações estranhas que não foram instaladas pelo utilizador, a alteração de configurações no telemóvel, bem como uma diminuição drástica no tempo de vida útil da bateria.

Alguns dos vírus que se encontram nos telemóveis têm como objetivo o roubo de palavras-passe dos utilizadores, autenticações bancárias, ou mesmo envio de mensagens e chamadas para números de valor acrescentado. Neste sentido, é importante que os utilizadores estejam atentos ao registo de chamadas e mensagens, à interrupção de chamadas sem motivo aparente ou a aumentos inexplicáveis do tráfego de dados.

BLUETOOTH

Se não formos cuidadosos, o Bluetooth pode ser um meio de invasão do nosso telemóvel. Se o deixamos sempre ligado, é possível a terceiros aceder sem autorização às informações que temos guardadas no nosso aparelho. Mas o que pode acontecer?

Bluebugging – os hackers assumem o controlo de um telemóvel através do auricular Bluetooth e utilizam-no para fazer chamadas, enviar mensagens de texto e aceder ao livro de endereços;

Bluejacking – são enviadas mensagens não solicitadas para dispositivos com Bluetooth, tais como telemóveis e tablets. É geralmente inofensivo, mas pode ser enviado conteúdo impróprio ou malicioso ou ainda tornarmo-nos vítimas de um intimidador;

Bluesnarfing – consiste em alguém aceder e copiar os dados pessoais armazenados num dispositivo Bluetooth, tais como livros de endereços, os nossos e-mails, mensagens de texto e fotografias, é a forma mais grave de invasão de privacidade.

SPIM / SPAM

Embora não sejam, por si só, um perigo, o SPAM (emails contendo informação/publicidade não solicitada) e SPIM (mensagens não solicitadas recebidas via instant messaging) podem ser extremamente incomodativos. Podemos receber inúmeros e-mails/mensagens que não nos interessam, a diversas horas do dia, que nos enchem a caixa de correio e ocupam memória do telemóvel. Contudo, tem em atenção que o SPAM/SPIM pode ainda conter tentativas de phishing, pelo que deverá tratar estas mensagens com cuidado e reserva. O melhor mesmo é eliminá-las.

Download de Apps

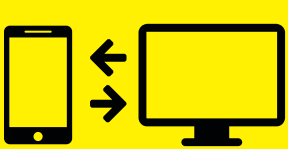
Uma grande percentagem dos ataques a telemóveis acontece por via do download de aplicações. Na sua grande maioria, o processo destes ataques passa por modificar uma aplicação legítima e popular no mercado e modificar o seu código de modo a que esta sirva os propósitos de uma conduta maliciosa. Estas aplicações tanto podem servir para deixar o teu telemóvel vulnerável a outro tipo de ataques, como para guardar registo de todas as tuas atividades com o telemóvel, capturando por exemplo, as tuas passwords.

WI-FI

Manter a ligação wireless continuamente ligada funciona como ter uma porta de entrada sempre aberta para o nosso smartphone e a informação que nele armazenamos. Isto acontece se temos selecionada no nosso telemóvel a opção de conectar automaticamente a redes, ou quando estamos a aceder a redes públicas ou redes que não estão protegidas.

QR CODES

Os códigos QR são uma maneira rápida e fácil para chegar aos websites a partir de um Smartphone ou um Tablet, utilizando a câmara do dispositivo. Como os códigos QR não podem ser lidos pelo olho humano, não sabemos para onde estamos a ser direcionados até entrar, correndo o risco deste ser um website fraudulento.



GEORREFERENCIAÇÃO

A maioria dos smartphones incluem tecnologia GPS que permite aos utilizadores partilhar a sua localização precisa em várias aplicações. No entanto, um "check-in" (partilha da localização atual) tanto pode ser visto por amigos, como por desconhecidos. Para além disso, se não prestarmos atenção às configurações do telemóvel, podemos partilhar a nossa localização ao publicar uma fotografia, sem nos apercebermos. Pode não ser boa ideia mostrar a toda a gente onde estamos.

O QUE PODES FAZER PARA ESTAR SEGURO?

* Proteger o nosso telemóvel com uma password. Esta é provavelmente a medida de segurança mais fácil de implementar e melhor obstáculo ao roubo.

* Devemos utilizar um antivírus no nosso telemóvel e fazer análises regulares ao conteúdo do nosso smartphone.

* Verificar se existem atualizações para o sistema operativo do nosso telemóvel e das aplicações que utilizamos. As atualizações trazem consigo novos pacotes de segurança contra os vírus mais recentes.

* É importante instalar software de limpeza remota de smartphones. Aplicações como o Find My Phone da Apple ou o Android Device Manager da Google permitem localizar o nosso telemóvel remotamente apagar tudo o que tem dentro.

* Devemos ter o cuidado de não clicar em links que são publicados nas redes sociais como o Facebook ou Twitter, mesmo quando publicados pelos nossos amigos.

NÃO CORRAS RISCOS

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

Microsoft

ipdj
INSTITUTO PORTUGUÊS DO DESPORTO E JUVENTUDE, I. P.

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE

ins@fe

Co-financiado pela Comissão Europeia
Programa Safer Internet

GOVERNO DE PORTUGAL
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

direção-geral educação