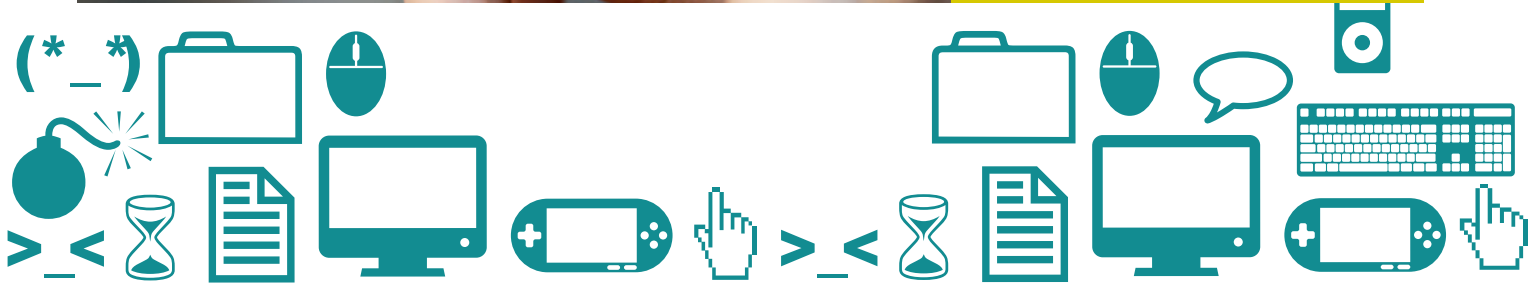
internet segura.pt

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". O aumento do número de serviços disponíveis num Smartphone tem sido exponencial e espera-se que estes continuem a aumentar. 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.

Como detetar um smartphone infetado?

Um smartphone, da mesma maneira que os computadores, é vulnerável a perigos como os do phishing, SPAM/SPIM, malware, roubo de informação pessoal e/ou de identidade e também cyberbullying. Assim, aplicam-se as mesmas regras de segurança.
Reconhece-se um smartphone infetado pela diminuição da performance, pelo aparecimento de aplicações que não foram instaladas pelo utilizador, pela alteração de configurações que não fizemos e ainda pela diminuição drástica da vida útil da bateria. É importante também estar atento à interrupção de chamadas sem motivo aparente ou a aumentos inexplicáveis do tráfego de dados.



A ter em atenção

Bluetooth e WI-FI
o Bluetooth e a WI-FI podem ser meios de invasão do nosso telemóvel. Se os deixarmos sempre ligados, é possível a terceiros aceder sem autorização às informações que temos guardadas no nosso aparelho.

Download de Apps
Ataques por download de aplicações são comuns. Na sua grande maioria, estes ataques passam por modificar uma aplicação popular no mercado para, por exemplo, deixar o telemóvel vulnerável a outro tipo de ataques ou guardar registo das atividades/informação do utilizador.

SPIM/SPAM
O SPAM (emails com informação/publicidade não solicitada) e o SPIM (mensagens não solicitadas recebidas via instant messaging) podem ser extremamente incomodativos e podem ainda conter tentativas de phishing, pelo que devemos tratar estas mensagens com cuidado.

QR Codes
Os códigos QR são uma maneira rápida e fácil de aceder a websites utilizando a câmara do telemóvel. Como os códigos QR não podem ser lidos pelo olho humano, podemos entrar num site fraudulento.

Georreferenciação
Os smartphones permitem partilhar a nossa localização precisa, por GPS, em várias aplicações. Essa partilha pode ser vista por amigos e desconhecidos. Se não prestarmos atenção às configurações do telemóvel, podemos partilhar a nossa localização com toda a gente.

O que podemos fazer para estar seguros?

Há algumas regras básicas que nos ajudam a garantir a segurança do nosso aparelho:

- Proteger o nosso telemóvel com password e ativar o autobloqueio para quando o telemóvel está inativo.
- Nunca fazer download de aplicações fora dos mercados próprios dos sistemas operativos (Google Play, App Store, Microsoft Store), uma vez que estes têm um controlo mais rigoroso.
- Evitar dar o número de telefone a desconhecidos ou disponibilizá-lo na Internet. Há empresas que recolhem os dados pessoais para os vender a terceiros e ainda indivíduos que os desviam para fins ilícitos.
- Não responder a mensagens ou chamadas de números desconhecidos. Muitas vezes, são esquemas de publicidade enganosa ou para cobrança de serviços de valor acrescentado.
- Utilizar um antivírus no nosso telemóvel e fazer análises regulares ao conteúdo do nosso smartphone.
- Manter o Bluetooth e WI-FI ligados apenas quando necessário e instalar todas as actualizações de segurança que sejam disponibilizadas pelo fabricante do telemóvel.
- Usar aplicações para a leitura de códigos QR disponíveis em fontes de qualidade reconhecida. Sempre que possível e especialmente em lugares públicos, devemos verificar se há indicações visuais de que um código QR foi adulterado (por exemplo, com um autocolante).
- Desativar a pré-visualização das mensagens. Pode ser útil ver mensagens com o telemóvel bloqueado, mas estamos a convidar as pessoas perto do telemóvel a lerem também a mensagem.
- 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. Isto é particularmente útil em caso de roubo, para ninguém ficar com a nossa informação.

LINHAAJUDA
internet segura.pt
808 91 90 90

Linha Alerta
internet segura.pt
linhaalerta.internetsegura.pt

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. Cuidado com mensagens do género «OMG nem vais acreditar no que acontece se clicares» ou «vê aqui a noite louca do Cristiano Ronaldo». É uma forma muito comum de passar malware e spyware.