Newsletter de Segurança

Millennium bcp

nº 47 Janeiro de 2009

Em destaque

O acesso ao Mobile Web através dos telemóveis de 3ª geração

Mais

Princípios básicos de segurança

Windows Mobile e Protecção de Dados

Mais

English version

Em destaque

O acesso ao Mobile Web através dos telemóveis de 3ª geração

Os telemóveis são já um equipamento essencial no nosso dia-a-dia. Com a chegada dos telemóveis de 3ª geração, o acesso à internet e a troca de conteúdos entre diferentes dispositivos passou a ser possível, de forma muito facilitada.

Desde que equipados para tal, esta nova geração de telemóveis permite aceder aos emails, fazer downloads ou visitar sítios da internet.

Trata-se de uma grande vantagem mas, à semelhança dos computadores, também tem os seus perigos. Convém, por isso, conhecer bem os riscos de aceder com o telemóvel à internet e as formas de prevenção dos mesmos, para que possamos tirar partido desta vantagem em segurança.

Como aceder à internet no telemóvel em segurança?

Um telemóvel, tal como um computador, poderá ser alvo de *phishing* ou SPAM (mensagens não solicitadas, que contêm informação variada ou publicidade).

Embora o SPAM por si só não constitua um perigo, pode, no entanto, conter acções de *phishing* pelo que se aconselha algum cuidado a abrir e tratar mensagens, sobretudo se remeterem para *links*. Estes *links* podem direccionar para páginas onde são solicitadas informações de carácter pessoal ou confidencial, cujo objectivo é recolher informação visando a sua eventual utilização maliciosa (as chamadas acções de *phishing*). Não introduza nunca as suas credenciais em sites que tenham origem

em *links*, faça sempre o acesso a esses sites através da digitação directa do endereço respectivo.

Utilizar o serviço Mobile Web em segurança

Para a utilização do serviço Mobile Web (mobile.millenniumbcp.pt), seja por telemóvel, Smartphone ou PDA apenas terá de:

- Ter acesso à internet (via GPRS, UMTS, Wi-Fi ou outros);
- Aceder a sites através de endereços seguros (https);
- Ter permissão de *cookies* activa.

Em relação ao acesso ao banco por via do Mobile Web, salientamos que:

- Todas as mensagens trocadas entre o telemóvel ou PDA do utilizador e o Millennium bcp são encriptadas, como tal, garantindo um nível de segurança acrescido;

- As mensagens circulam na rede através de linhas dedicadas e de canais de comunicação seguros e encriptados;

- Para aceder às suas contas através do Mobile Web, terá de indicar o seu Código de utilizador, o mesmo que utiliza quando acede ao portal Millennium bcp (www.millenniumbcp.pt) a partir de um computador, o seu mutlticanal ou password completa e duas posições aleatórias de um documento de identificação;

- Todas as operações bancárias, que não sejam consultas, necessitam de validação através da indicação de 3 dígitos da Chave de Confirmação, que deve ser, apenas, do seu conhecimento.

- Deve alterar regularmente a sua Chave de Confirmação na opção Contas>Personalização>Códigos de Acesso. Caso necessite de uma Chave de Confirmação, poderá solicitar após o login no site, seleccionando o item Personalização > Códigos de Acesso > Pedir Chave de Confirmação.

Fonte: millenniumbcp.pt

Topo

Princípios básicos de segurança
Windows Mobile e Protecção de Dados

À data de hoje, existem mais de 200 telemóveis diferentes provenientes de 56 fabricantes de *hardware*, utilizados por 160 operadores móveis em tudo o mundo. Existem, ainda, mais de 18 mil aplicações Windows Mobile disponíveis para esta plataforma.

Em Portugal, o número de aparelhos de comunicações móveis já ultrapassou o número da população total.

Esta é uma realidade que veio para ficar. E que preocupações deveremos ter no respeitante à segurança e protecção de dados, quando se utiliza um aparelho de comunicações móveis?

Face à crescente capacidade de processamento e de armazenamento nestes aparelhos, cada vez é possível fazer mais: ter acesso ao correio electrónico, seja ele pessoal ou profissional; aceder à Internet; comunicações em tempo real; jogos; música; fotografia; *software* de produtividade, enfim, um sem número de possibilidades.

Quanto maior o uso, maiores deverão ser os cuidados a ter em conta na utilização deste tipo de aparelhos, sobretudo quando utilizados em ambientes profissionais.

Assim, deverá ter em consideração as seguintes precauções:

- Ao navegar na Internet através de um aparelho de comunicação móvel, deverá ter exactamente os mesmos cuidados que tem quando navega no computador, tais como, não visitar sites de natureza duvidosa ou não aceitar seguir *links* que não pediu.
- Porque é fácil perder o telemóvel, é aconselhado activar a funcionalidade de bloqueio automático ao fim de algum período de inactividade, de modo a impedir o acesso fácil à informação que esteja armazenada no mesmo. Se necessita de ter informação confidencial armazenada nestes aparelhos, deverá, ainda, ter em consideração outros pormenores na área de segurança. A possibilidade de desabilitar determinadas funcionalidades de *hardware* como a câmara ou a ligação *bluetooth* ou a capacidade de, remotamente, limpar todo o conteúdo que se encontra no aparelho, são alguns exemplos. Estas funcionalidades são disponibilizadas pelo Windows Mobile. Outra funcionalidade disponibilizada pelo Windows Mobile tem a ver com a possibilidade de juntar os aparelhos com Windows Mobile à infra-estrutura de directório da empresa. Esta é, sem dúvida, uma funcionalidade que proporciona mais segurança uma vez que tornar-se-á mais fácil implementar políticas centralmente, tais como a encriptação dos dados armazenados.

Visto que a camada mais jovem da sociedade é utilizadora de telemóveis, recomendamos a leitura do Acordo-quadro europeu para a utilização mais segura dos telemóveis pelos adolescentes e crianças, disponível em http://www.gsmworld.com/gsmeurope/documents/eur.pdf.

Neste documento encontramos boas práticas que devem ser tidas em conta para uma utilização dos telemóveis mais segura para todos.

Fonte: Microsoft

Topo

Security Newsletter

nº 47 January 2009

Highlights

Mobile Web access on third generation mobile phones

More

Basic security principles

Windows Mobile and Data Protection

More

Versão portuguesa

Highlights

Mobile Web access on third generation mobile phones

Mobile phones are essential day-to-day equipment. 3G mobile phones have made it much easier to go online and to exchange content between different devices.

If properly equipped, this new generation of mobile phones allows you to access your email, download files or visit sites over the internet.

These advantages, like for the PC, come with some danger. That's why it's so important to learn about the risks of using your mobile phone to connect to the internet and how to avoid them - to be able to use these advantages in a secure manner.

How to securely access the internet over my mobile phone

A mobile phone, just like a PC, can be the target of phishing or spam (unwanted email messages or advertising).

Although spam doesn't of itself constitute a danger, it can, nevertheless, be a vehicle for phishing. It's therefore important to take care when opening and handling emails, especially if they contain links. Such links may direct you to webpages that ask you to enter personal or confidential information. The goal is to collect information for possible malicious use (phishing). Never enter your details or passwords in websites originating from links. Always access sites by entering the address directly in your browser.

Using the Mobile Web service securely

To use the Mobile Web service (mobile.millenniumbcp.pt), be it by mobile phone, Smartphone or PDA, you simply need to:

- Have internet access (via GPRS, UMTS, Wi-Fi or other);
- Access websites with secure addresses (https);
- Accept cookies from sites.

As for accessing the bank over the Mobile Web, please note that:

- All messages exchanged over your mobile phone or PDA and Millennium bcp are encrypted to ensure an additional level of security;

- Messages circulate within the network on dedicated lines and secure and encrypted communication channels;

- To access your accounts over the Mobile Web you have to enter your User Code - the same you use when you access the Millennium bcp website (www.millenniumbcp.pt) from a PC -, your full multichannel code or password and two random positions of a personal identification document;

- All banking operations (excluding viewing your accounts) require validation - 3 digits from your confirmation key (which should only be known to you);

- You should regularly change your Confirmation Key under Accounts>Customisation>Access Codes. If you need a Confirmation Key, you may request one after having logged into the site by selecting Customisation > Access Codes > Request Confirmation Key.

Source: millenniumbcp.pt

Top

Basic security principles

Windows Mobile and Data Protection

There are currently over 200 different mobile phone models from 56 hardware manufacturers in use by 160 mobile operators across the globe. What's more, there are over 18,000 Windows Mobile software applications available for this platform.

There are more mobile communication devices in Portugal than there is total population.

This is a reality that has come to stay. And what measures should we take regarding the security and data protection of mobile communications devices?

In light of their increasing capacity to store and process data, every day it's easier to: access your personal or work email; surf the internet; chat in real time; play games; listen to music; take photos; use software to improve your productivity, etc... an endless number of possibilities.

The more we use these devices, the greater the care we must take, especially when we use them for working.

You must keep the following precautions in mind:

- When surfing the web over a mobile communications device, you must be just as careful as when on a PC - don't visit dodgy sites or follow links you haven't requested.

- Since it's not that hard to lose a mobile phone, you should set it to automatically block itself after a certain period of inactivity to prevent others easily accessing your information. If you need to store confidential information on it, you should also take other security measures into account. You can, for example, turn off certain hardware functions such as your camera, Bluetooth connection, or the possibility of remotely deleting all your content. Such functions are made available by Windows Mobile. Another function Windows Mobile gives you access to is the possibility of connecting Windows Mobile devices to your company folder infrastructure. This is a function that will undoubtedly enhance security since it makes it easier to centralise security policies, such as the encryption of stored data.

Since the younger part of our society uses mobile phones, we recommend you read the European framework agreement for Safer Mobile Use by Younger Teenagers and Children, available at http://www.gsmworld.com/gsmeurope/documents/eur.pdf.

Here you can find good practices for a more secure use of mobile phones.

Source: Microsoft

Top

Best Consumer Internet Bank
Best Integrated Corporate Bank Site