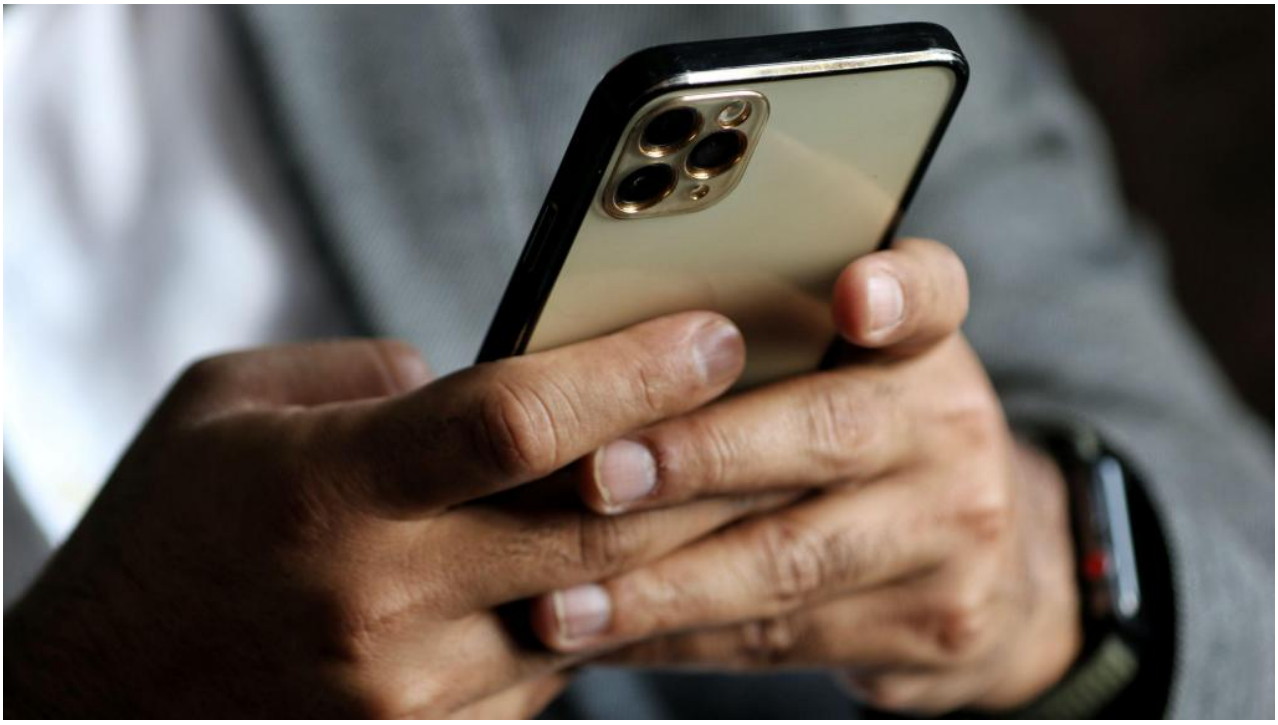
Aplicações, e-mails e homebanking: da espionagem ao roubo de dinheiro, saiba como estar protegido

cnnportugal.iol.pt/whatsapp/email/aplicacoes-e-mails-e-homebanking-da-espionagem-ao-roubo-de-dinheiro-saiba-como-estar-protegido/20230514/645d117fd34ea91b0aac664b

João Guerreiro Rodrigues , JGR
Ontem às 12:35



Utilizamo-las todos os dias com uma confiança quase cega, mas as nossas aplicações podem não ser tão seguras quanto pensamos

Cada vez mais presente no nosso dia-a-dia, a tecnologia trouxe consigo uma nova onda de conveniência, mas também de insegurança. Todos os dias, comunicamos com família e amigos, enviamos e-mails aos nossos colegas de trabalho, utilizamos o nosso homebanking e guardamos no nosso telemóvel fotografias e vídeos que jamais gostaríamos que vissem a luz do dia. Tudo isto porque assumimos que estas aplicações são seguras – mas nem sempre assim. Saiba ao que deve estar atento e como se pode proteger.

Whatsapp

Um dos principais erros que as pessoas cometem quando utilizam uma aplicação é presumir que esta, simplesmente por estar disponível, é completamente segura. O Whatsapp é uma das plataformas mais vulneráveis a esta presunção, porque muitos dos seus utilizadores acreditam que o sistema de mensagens encriptadas é inviolável e só os intervenientes é que têm acesso às mesmas. Além de poder ser alvo de casos de

hacking, com especialistas informáticos a conseguir quebrar o código de encriptação do serviço, os metadados destas mensagens podem ser vulneráveis a intrusão ou a vigilância por parte de terceiros capazes de o fazer.

“A comunicação de voz do Whatsapp é encriptada, mas a estrutura que suporta a aplicação guarda toda a sua informação e essa infraestrutura não é infalível”, explica Bruno Castro, especialista em cibersegurança e CEO da VisionWare.

Os especialistas alertam também que um dos erros mais comuns que as pessoas praticam está na etiqueta de utilização. Não carregue em todos os links que recebe, particularmente de pessoas com quem não mantém contacto frequente, mesmo que conheça há muitos anos. Esse seu contacto pode ter sido infectado por um vírus que está a ser reencaminhado para si.

“As pessoas precisam de ter muitos cuidados no que toca às mensagens de Whatsapp. Muita atenção aos links, particularmente em grupos. Os links, às vezes, executam pequenos pedaços de código no nosso telefone que podem levar a problemas no futuro”, afirmou Nuno Mateus Coelho, especialista em segurança informática.

E-mail – não se esqueça da etiqueta

O email é uma forma útil e conveniente de comunicar, mas nem sempre é segura. Saiba que os emails podem ser intercetados e os utilizadores devem sempre evitar enviar informação sensível por esse meio. Os especialistas sugerem que encare o seu email como se da sua morada física se tratasse, por isso, evite a sua exposição desnecessária.

“Muitas pessoas ainda têm a má prática de enviar emails para grupos colocando os seus endereços todos na lista de contactos para quem enviar, em vez de os pôr em ‘bcc’. Exposição do email é algo sensível, porque cada vez mais somos atacados por email. Tem de ser encarado quase como se fosse a nossa morada física”, frisa Bruno Castro.

Nos dias que correm, o phishing continua a ser uma das forças favoritas de ataque por parte de piratas informáticas. Esta técnica é fácil de executar e permite aos intrusos enviar mensagens para milhares de contactos com links que podem conter ameaças à sua segurança. Tenha uma atenção redobrada quando recebe emails com links ou com anexos. Procure erros gramaticais ou possíveis sinais de veracidade antes de carregar em qualquer sítio.

Pode parecer básico, mas é sempre importante recordar a “etiqueta” e utilizar passwords o mais completas possível, com um misto de letras maiúsculas e minúsculas, números e símbolos, bem como ativar um sistema de autentificação dois fatores. Se a confidencialidade da sua mensagem é algo que lhe preocupa, vá um passo mais longe e procure utilizar sistemas de encriptação de email ou email que já possuem esse serviço.

Homebanking

O serviço de homebanking tornou-se algo cada vez mais presença na vida dos portugueses e os piratas informáticos sabem disso. Apesar de ser um serviço bastante seguro, não está livre da sua maior vulnerabilidade: o próprio utilizador. Por isso, é bastante importante ativar a autenticação de dois fatores para proteger as suas informações financeiras. Certifique-se também que aplicação que instalou é mesmo fidedigna ou que o link do site corresponde mesmo ao endereço autêntico.

“Quando somos vítimas de um ataque orientado por parte de um hacker, os nossos dispositivos podem estar infetados para esconder as nossas notificações SMS e enviá-las para outro dispositivo (do atacante). Se o atacante tiver os códigos, consegue receber o SMS e dar o ok à operação”, diz Nuno Mateus Coelho.

É também importante recordar o básico: o seu banco nunca vai pedir as suas credenciais ou informações pessoais por e-mail ou por telefone, por isso, não as forneça a ninguém. Além disso, desligue a conta sempre que acabar de utilizar o serviço.

Cartão de Crédito

A tendência era imparável, mas desde a pandemia de covid-19 que as compras online passaram a ser cada vez mais uma parte dos nossos dias. Mas com ela vieram riscos acrescidos e mais terreno para que piratas informáticos consigam roubar os nossos dados do cartão de crédito. Um dos erros mais comuns apontado pelos especialistas é a utilização de uma rede de Wi-fi pública ou não segura. Conexões Bluetooth e Wi-Fi abertas podem ser exploradas por hackers que desejam aceder ao seu dispositivo. Certifique-se que desativa essas conexões quando não estão em uso, de forma a evitar essas ameaças de segurança.

“Não há mal em utilizar redes públicas, mas é importante segregar o tipo de informação a que acedemos. Uma coisa é ver sites de informação ou ir às redes sociais, outra coisa é aceder ao meu homebanking ou ao meu email através de redes que eu não tenho a certeza que são seguras”, explica Bruno Castro.

Outros dos erros mais comuns passa por não verificar com frequência o seu registo de movimentações. Mesmo tendo mecanismos de deteção de transações suspeitas, nem sempre estes são acionados e você pode dar por si e ter diversos pagamentos não autorizados.

Não deixe que a conveniência ponha em causa a sua segurança e do seu dinheiro. Evite guardar os dados bancários no seu dispositivo móvel. Sim, é muito mais fácil de utilizar, mas é também muito mais arriscado. Se alguém conseguir obter acesso ao seu dispositivo, essa pessoa poderá conseguir utilizar a informação do seu cartão de crédito para levar a cabo compras indesejadas. Aqui é preferível utilizar, se possível, palavras-passe biométricas como a impressão digital ou o reconhecimento facial.

“Guardar passwords é um erro que já não se admite, nos dias de hoje. Os serviços dos bancos até são bastante robustos, porque é uma área onde se investiu muito, mas os ataques são na generalidade focados na pessoa a quem se quer roubar as credenciais”,

refere o CEO da VisioWare.

Aplicações

Utilizamos tantas que às vezes até nos acabamos por esquecer delas algures no nosso telemóvel, mas deve ter muita atenção, porque pode estar a convidar um intruso para o seu dispositivo. Não descarregue aplicações de sítios não oficiais. Utilize sempre o Google Play ou a Apple App Store para proteger o seu dispositivo. Ainda assim, deve fazer o seu "trabalho de casa" e olhar para o que outros utilizadores escrevem acerca da aplicação que pretende descarregar.

"É importante verificar sempre a reputação de uma aplicação que queremos descarregar. Temos mesmo de ter uma rotina de segurança no nosso telefone", insiste o especialista.

Com o passar do tempo, é normal que sejam descobertas vulnerabilidades nos códigos de uma aplicação. Por isso, é essencial que você atualize com frequência as aplicações que descarregou. Os programadores destas empresas trabalham com regularidade para corrigir erros ou falhas que permitem o seu dispositivo ser atacado por piratas informáticos.

Tenha também uma atenção redobrada às permissões que dá às aplicações instaladas no seu telemóvel. Muitos destes serviços ganham dinheiro a vender os seus dados e, para isso, requisitam acesso à sua localização, ao seu microfone e à sua câmara, por exemplo. Verifique com atenção, nas definições do seu telemóvel, as permissões que dá a cada uma delas.

Fotos e vídeos

Não parta do princípio que o seu dispositivo é totalmente seguro. Tal como as suas aplicações podem ser alvo de ataques, o mesmo acontece com a restante informação que tem no telemóvel. Por isso, é importante fazer backups regulares para a cloud ou para um dispositivo de armazenamento externo.

É fundamental não partilhar os acessos ao seu telemóvel com ninguém, nem mesmo com pessoas que lhe são próximas. Muitas vezes são essas próprias pessoas que acedem sem o seu consentimento às suas informações. É isso que acontece com o chamado stalkerware, um software malicioso que é instalado sem o conhecimento no dispositivo da vítima e é utilizado para rastrear e monitorizar toda a atividade do mesmo, incluindo chamadas, mensagens, localização e histórico de pesquisas. É frequentemente usado por indivíduos que pretendem controlar os seus parceiros ou outras pessoas sem o seu conhecimento. Além disso, limite o acesso físico que outros têm ao seu smartphone, especialmente pessoas em quem não tem confiança.

Não dê como garantida a segurança do seu smartphone só porque tem um antivírus inteligente instalado. Se quisermos ter a certeza de que temos o nosso equipamento seguro, devemos fazer uma verificação um pouco mais exaustiva. Desative o acesso ao

microfone a todas as aplicações que não usam o microfone, exceto durante a utilização. O mesmo acontece com a câmara e com a localização.

“Devemos fazer o que eu chamo 'higienizar o sistema' - desativar o acesso ao microfone a todas as aplicações que não usam o microfone. O mesmo acontece com a localização e com a câmara. Estas aplicações vendem os nossos dados a empresas terceiras”, explica Nuno Mateus Coelho.

Temas: Whatsapp Email Segurança Hackers Hacking