Cibersegurança

Guia de boas práticas

Abreu advogados

Índice

Social Engineering

É uma técnica utilizada para uma vasta gama de atividades maliciosas realizadas através da interação humana. Utiliza a manipulação psicológica para enganar a vítima, levando-a a cometer erros de segurança ou a partilhar informação sensível.

Vetores de ataque normalmente utilizados:

• Utilizando um isco, chamando a atenção, a curiosidade ou ingenuidade da pessoa;

• Utilizando o medo, fazendo com que a vítima se atrapalhe ou fique receosa de que algo mau acontecerá;

• Utilizando pontos de referência ou linguagem semelhante à do trabalho;

• Passando um sentido de urgência/emergência na comunicação.

Via texto (SMS, E-mail)	**Via chamada**
Olá, esta é uma mensagem automática do IT, responda a esta com a sua password para desbloquear o seu utilizador caso contrário irá perder acesso ao sistema dentro de 5 minutos.	- Estamos a ligar pois tivemos um erro no sistema. Poderia, por favor, dizer-me a sua identificação e senha para reconciliar os dados salariais corretamente?

Como prevenir:

- Não responda a e-mails nem mensagens de números que não sejam de contactos conhecidos;

- Suspeite quando existem promessas ou ofertas;

- Não abra links ou anexos que sejam recebidos de fontes externas sem saber se são seguros;

- Leia sempre com calma e com rigor crítico, independentemente do teor de urgência da mensagem.

Mensagens (SMS) e chamadas

À semelhança do que vemos nos e-mails de Phishing, no caso dos SMS e chamadas, somos contactados por números anónimos, ou por contactos fraudulentos, que se fazem passar por entidades fidedignas.

A mensagem de texto, tipicamente, pedirá para clicar num link para “verificar”, “atualizar” ou “reativar” a conta ou até mesmo proceder a algum tipo de pagamento, mas, na realidade, o link redireciona para uma página falsa e o número de telefone liga ao Hacker, fingindo ser uma empresa verdadeira.

Cuidados a ter neste tipo de ataque:

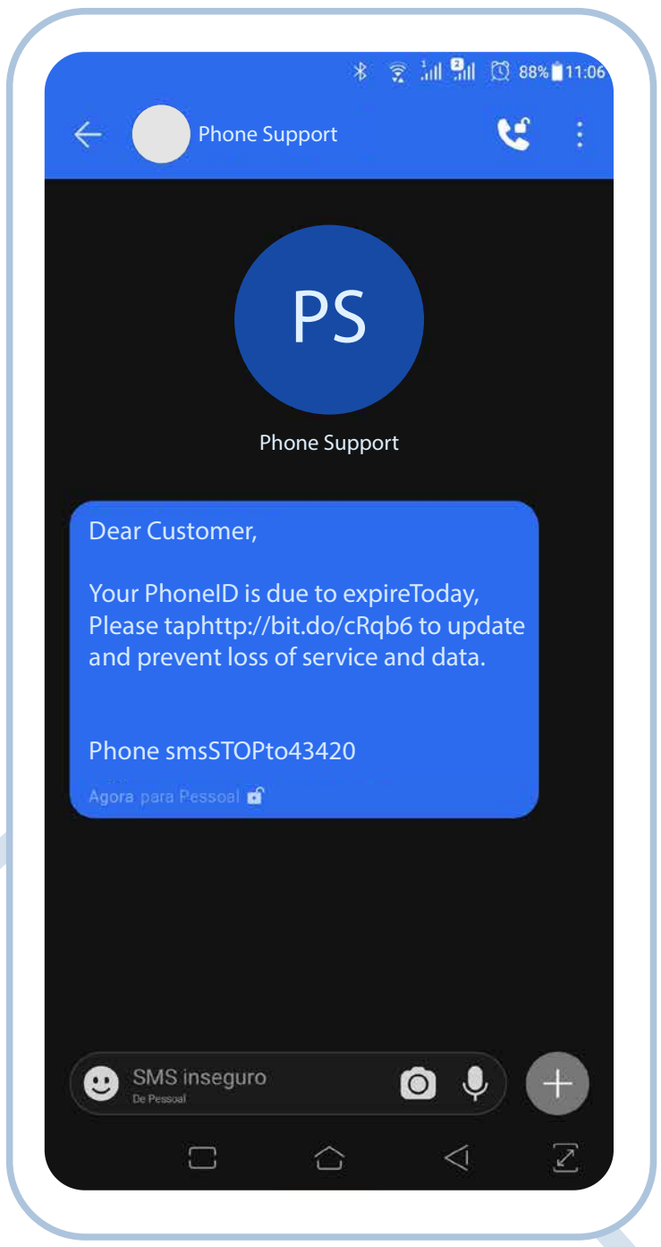
• Não carregue em links, anexos ou imagens que receba em mensagens de texto não solicitadas, sem verificar quem as enviou;

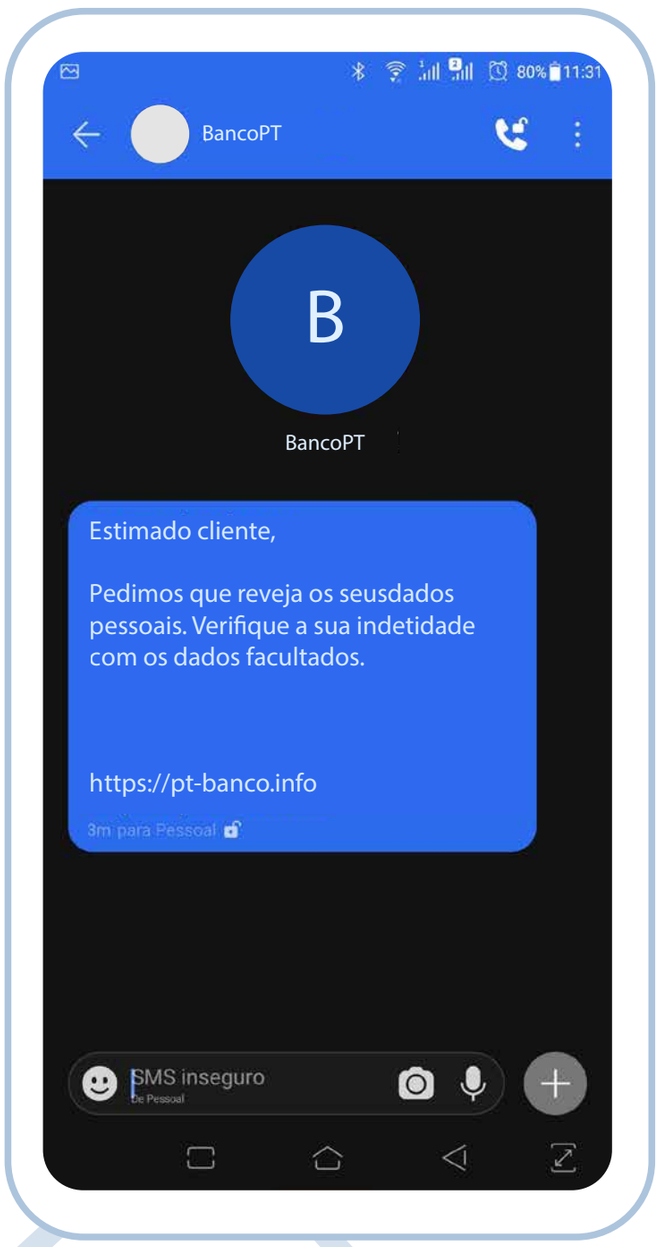
• Não deixe que o “apressem” - verifique calmamente tudo o que precisa antes de responder;

• Encare como suspeitas mensagens contendo: "Parabéns, você ganhou", "A sua encomenda encontra-se retida" e "Responda agora";

• Nunca responda a mensagens de texto que lhe peçam pins, passwords de acesso ou outros dados sensíveis.

Exemplos:





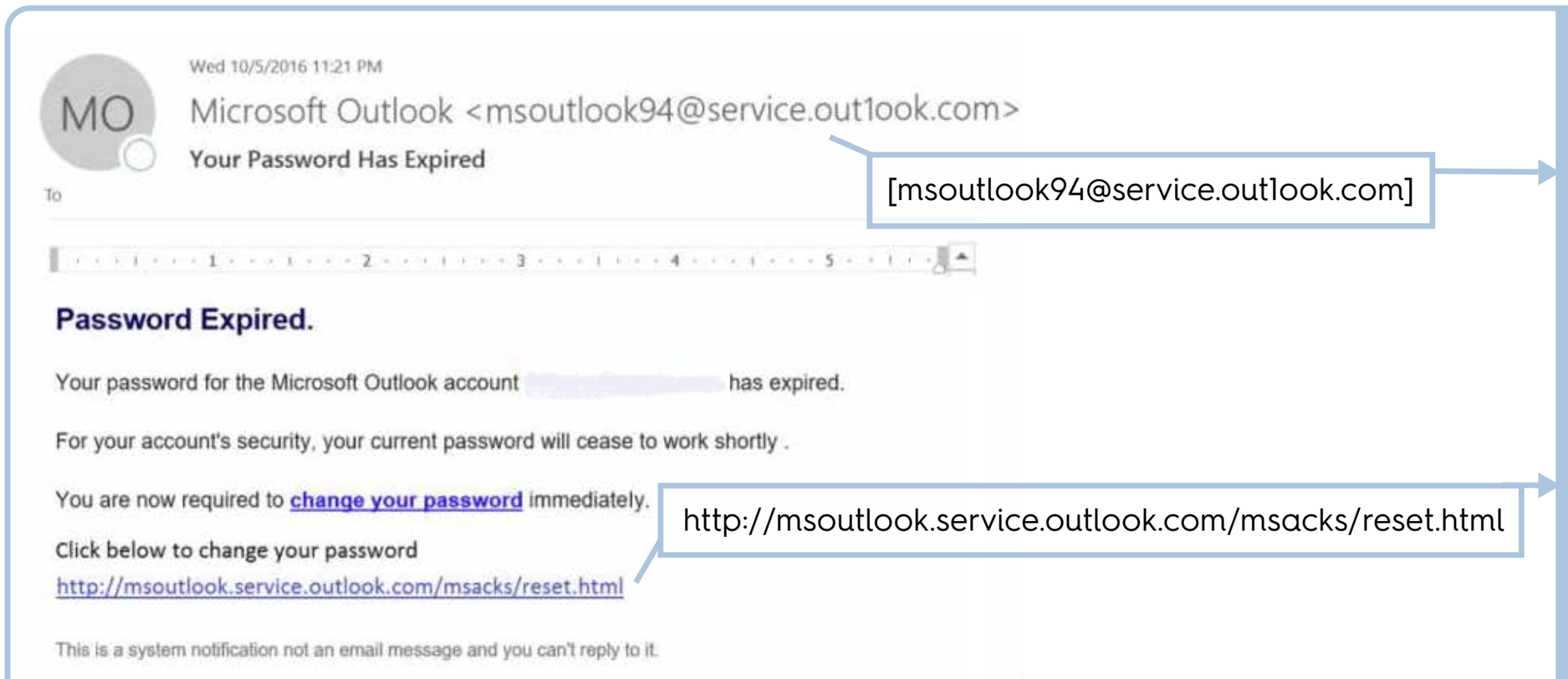
E-mail

Este é o ataque mais comum e com que estamos mais familiarizados.

Um dos métodos usados é a utilização de emails idênticos aos da própria empresa, com a mesma identidade gráfica, logótipos e mensagens reais.

Tipicamente transmitem urgência e pedem para descarregar um anexo ou clicar num link que nos direciona para uma página falsa, que serve para roubar informação pessoal.

Exemplo:



Perigos na navegação da internet

Um website malicioso é aquele que tenta instalar malware, um termo genérico para qualquer coisa que perturbe o funcionamento do computador, que recolha informações pessoais ou, na pior das hipóteses, que obtenha ou permita obter acesso total à máquina, sendo para isso necessário alguma ação da nossa parte.

Muitas vezes os websites maliciosos assemelham-se aos legítimos, para nos dar uma falsa sensação de confiança e para, eventualmente, nos pedirem para submeter credenciais ou informação sensível.

Como nos podemos prevenir?

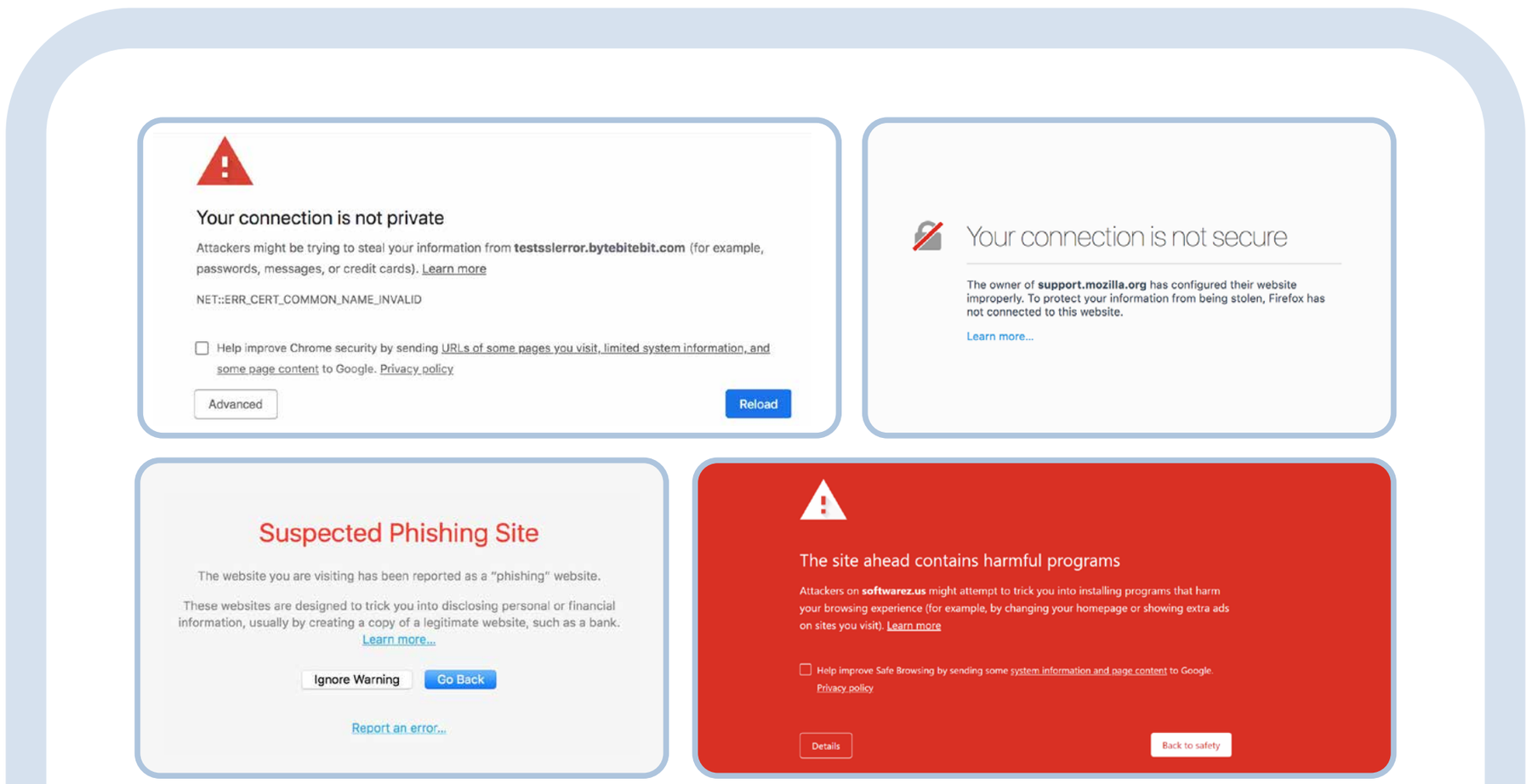
O antivírus nem sempre consegue detetar malware de sites maliciosos, no entanto, pode impedir a sua abertura, caso sejam descarregados por engano, avisando-nos sempre que algum conteúdo perigoso ou suspeito foi bloqueado.

A melhor coisa que pode fazer para se proteger é manter o software e, sobretudo, o sistema operativo do computador atualizados. Muitas vezes, os hackers utilizam problemas de segurança conhecidos no software, antes que os fabricantes possam corrigir a falha. A atualização do seu software impede-o de ser um "low hanging fruit".

Quando está a lidar com informação litigiosa, como acessos bancários, a melhor prevenção é estar atento enquanto utiliza a internet.

Se um website parecer suspeito e tentar instalar algo, pedir permissão para tal ou descarregar ficheiros autonomamente, o melhor é fechar o separador.

Exemplos:



Links e anexos maliciosos

Nos dias que correm, os ataques por correio eletrónico são apenas um dos vários mecanismos usados por Hackers para os seus ataques. Abaixo indicamos outros meios utilizados para tentar extrair informação.

Boas práticas no uso de passwords

Uma das formas mais comuns que os hackers usam para invadir os computadores é adivinhando passwords, utilizando “bots” (aplicações autónomas) que fazem um número alto de combinações por segundo. As senhas simples e frequentemente utilizadas permitem, aos intrusos, obter facilmente acesso e controlo de um dispositivo informático.

Ao aumentar a complexidade da sua password, faz com que este tipo de ataques não seja viável, tendo em conta o tempo que seria necessário para a quebrar. Quanto mais difícil for a palavra-passe, menor será a probabilidade de o computador ser vítima de uma intrusão indesejada.

Como podemos reforçar as nossas passwords?

Incluindo os parâmetros que já conhecemos:

• No mínimo catorze caracteres;

• Utilizar maiúsculas e minúsculas;

• Adicionar números, sinais de pontuação e caracteres especiais (exemplos: "!", ".", "_", "@", "€", "£");

Considerando o elevado número de passwords de que precisamos hoje em dia, é cada vez mais difícil geri-las a todas. Neste sentido, se queremos garantir a sua complexidade e segurança, precisamos de arranjar mecanismos que nos ajudem nesta tarefa. Uma forma simples de criar uma password segura é memorizar uma frase e ir alterando alguns caracteres, utilizando os parâmetros mencionados.

Cuidados a ter:

• Evitar o uso de informação pessoal (como o nome, data de nascimento, etc..);

• Alterar periodicamente as passwords, não repetindo as últimas 4;

• Alterar as passwords com uma periodicidade não superior a 90 dias;

• Não utilizar a password da sua empresa em outros locais;

• Não gravar credenciais nos browsers;

• Utilizar, sempre que possível, autenticações de dois fatores - por e-mail, SMS, token, etc. -, uma vez que estas aumentam consideravelmente a segurança da conta.

Boas práticas em equipamentos de armazenamento externo

A maior parte das pessoas assume que os dispositivos de armazenamento externo (pens USB, CD's e discos externos) são seguros, mas a realidade é que podem ser utilizados para realizar ciberataques. O simples ato de ligar uma pen USB ao computador pode fazer com que sejamos vítimas de um ciberataque.

Como evitamos ser vítimas de um ciberataque destes?

Não devemos ligar equipamentos de armazenamento desconhecidos ao nosso computador.

Não devemos ligar os nossos equipamentos de armazenamento a computadores desconhecidos, como computadores públicos, porque poderão ficar infetados e, mais tarde, propagar o vírus na sua máquina.

Segurança em dispositivos móveis

A segurança deve ser tida em conta durante todo o ciclo de vida do dispositivo: desde a escolha do dispositivo, à manutenção das condições de segurança do mesmo (updates de sistema), ao controlo dos dados e, finalmente, à formatação do dispositivo antes de qualquer destruição ou entrega a terceiros (apagando todos os dados nele contidos).

- **Pretendo formatar/eliminar a informação de uma PEN USB previamente utilizada**

Quando falamos em formatação, para eliminar todos os conteúdos com segurança que se encontram na PEN USB não basta eliminar os mesmos. Existe forma de recuperar essa informação "eliminada", para que não seja possível é utilizado um software próprio que elimina de forma permanente os dados da PEN USB.

- **Não deixar os equipamentos / dados desprotegidos**

Uma falha crítica de segurança tem que ver com os dados que deixamos acessíveis a todos, como deixar passwords escritas em locais expostos ou deixar o computador desbloqueado em locais públicos.

Perigos na utilização de redes wifi desconhecidas / públicas

Os acessos públicos de wifi encontram-se em diversos sítios conhecidos: aeroportos, cafés, centros comerciais, restaurantes, hotéis, entre outros. Estes acessos são tão facilitados e divulgados que, por norma, acedemos sem pensarmos duas vezes. Embora pareça inofensivo, fazermos login para vermos as redes sociais, consultarmos as noticias ou o e-mail pode representar um perigo nestas redes públicas.

O problema com o wifi público é que existe um número enorme de riscos que acompanham estas redes. Embora os proprietários das empresas possam acreditar que estão a fornecer um serviço valioso aos clientes, é provável que a segurança nestas redes seja fraca ou inexistente.

Cuidados a ter:

• Em redes Wi-Fi desconhecidas, principalmente locais públicos como cafés, hotéis ou mesmo Wi-Fi gratuita no centro comercial/metro, é recomendado utilizar um serviço de VPN para assegurar a integridade e sigilo da informação durante a utilização da internet;

• Visitar apenas websites utilizando HTTPS (ex: https://www.abreuadvogados.com);

• Fazer logoff de contas após acabarmos de as utilizar;

• Não deixar a opção “auto-connect to wifi” ligada;

• Desligar o wifi ou bluetooth se não estiverem a ser utilizados;

• Não ligar a redes wifi que não sejam protegidas por password.

É nossa recomendação que apenas utilizem estes acessos em casos extremos e onde não haja mais nenhuma alternativa, dando sempre prioridade ao uso de dados móveis. Abaixo, deixamos alguns exemplos de possíveis ataques que podem ser feitos em redes públicas.

• Snooping and sniffing

Esta técnica permite aos atacantes acederem a tudo o que estiver a fazer online, desde ver páginas web que tenha visitado (incluindo qualquer informação que possa ter preenchido enquanto acedia a essa página web), até serem capazes de captar as credenciais de login, comprometendo a conta e os dados nela contidos.

• Malicious hotspots

Estes hotspots enganam as vítimas para se ligarem ao que pensam ser uma rede legítima, porque o nome parece “respeitável”. Digamos que está hospedado num Hotel e quer ligar-se à rede wifi do hotel. Pode pensar que está a selecionar a rede correta quando clica em "Wi-fi Hotel", mas, em vez disso acabou de se ligar a um malicious hotspot criado por terceiros, que agora podem ver a sua informação.

Nota: Confirmar sempre com a receção (ou equivalente) o nome da rede e acessos antes de usar.

Malware distribution

Graças às vulnerabilidades de software, há também formas de os atacantes poderem introduzir malware no computador de forma despercebida. Uma vulnerabilidade de software é uma falha ou fraqueza de segurança encontrada num sistema operativo ou num programa. Os hackers podem explorar esta fraqueza escrevendo código e depois atingir uma vulnerabilidade específica para depois injetar código malicioso no seu dispositivo.

Man-in-the-Middle attacks:

Essencialmente, um ataque MitM é uma forma de espionagem. Quando um computador faz uma ligação à Internet, os dados são enviados do ponto A (computador) para o ponto B (serviço/site) e as vulnerabilidades podem permitir ao atacante intercetar estas transmissões e "lê-las". Assim, o que se pensava ser privado já não o é.

Conheça a nossa equipa de Proteção de Dados Pessoais e Cibersegurança

A Abreu Advogados tem uma equipa dedicada e especializada em temas de privacidade e segurança da informação. Através do nosso Serviço Proteção de Dados Pessoais e Cibersegurança oferecemos soluções que asseguram a conformidade com a legislação aplicável em matéria de proteção de dados pessoais e Cibersegurança.

Gerimos projetos direcionados à verificação de conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e demais legislação aplicável, à avaliação de impacto na proteção de dados pessoais, bem como à avaliação de riscos inerentes à Cibersegurança, quer no âmbito estritamente legal, quer na perspetiva técnica, nestes casos, em parceria com entidades com as quais estabelecemos parcerias para o efeito.

O nosso trabalho tem abrangido uma diversidade de clientes, desde grandes clientes multinacionais, a pequenas e médias empresas nacionais, guiando-os nas auditorias – avaliando o modo como recolhem, tratam e protegem os dados pessoais de clientes, trabalhadores e terceiros com os quais se relacionam – prestando aconselhamento na gestão diária de questões de privacidade, nomeadamente na sua conformidade com as orientações emitidas pela entidade reguladora portuguesa.

A nossa atuação proporciona uma cobertura integral de todas as áreas substanciais relacionadas com a privacidade e segurança de dados, fruto da nossa experiência com clientes de uma grande variedade de empresas líderes em vários sectores, incluindo bens de consumo, banca e serviços financeiros, serviços de saúde, serviços de internet, farmacêuticas, telecomunicações, etc.

Em concreto, os nossos serviços concretizam-se nos seguintes temas: Auditorias iniciais e de verificação regular; Litigância em matéria de proteção e segurança dos dados; Privacidade nos recursos humanos; Avaliação de impacto de novas tecnologias; Cibersegurança; Transferências transfronteiriças de dados.

Ricardo Henriques
Sócio da Abreu Advogados

ricardo.henriques@abreuadvogados.com

Simão de Sant'Ana
Sócio Contratado da Abreu Advogados

simao.santana@abreuadvogados.com

Thinking about tomorrow?
Let's talk today.

Abreu:
advogados