Guia de Segurança

Check List de leitura rápida
Secure Remote Working

claranet cyber security

Trabalhar remotamente de forma segura

Muitos de nós estamos agora a trabalhar agora a partir de casa e, felizmente, na maioria dos casos, sem problemas de segurança. No entanto, trabalhar remotamente significa que temos de assumir uma responsabilidade extra em relação à segurança. A probabilidade de um ataque é maior (regra geral, um e-mail de **phishing**) e as dispendiosas medidas de defesa do escritório não estão lá para nos proteger.

Seguem-se alguns passos simples que podemos empregar para garantir que permanecemos seguros quando trabalhamos remotamente:

Está a usar o seu próprio computador ou portátil?	Se estiver a usar um dispositivo facultado pela sua empresa, provavelmente já terá um software antivírus. Se estiver a usar o seu próprio dispositivo, deve certificar-se de que mantém o seu antivírus atualizado. Se estiver a usar o Windows, o Microsoft Defender é uma opção perfeitamente adequada, existindo várias versões gratuitas disponíveis na internet. Além disso, muitos sistemas operativos antigos já não recebem suporte, encontrando-se, por isso, numa situação vulnerável. Certifique-se de que uma versão mínima do sistema operativo está a ser usada. O XP e o Windows 7 já não devem ser usados, por exemplo.
Wi-Fi pública	Sempre que possível, não utilize a rede Wi-Fi pública. Se tem de usar uma rede Wi-Fi pública, certifique-se de que usa uma **VPN** para evitar que os seus dados sejam espiados e roubados.
Utilize *passwords* fortes	Não use a mesma password para tudo. A reutilização de passwords é a primeira coisa que um atacante vai procurar. Usar a mesma password para aceder a todas as suas redes sociais e entrar no seu banco e rede significa que, se o atacante descobrir isto, poderá aceder a todo o seu mundo privado. Os gestores de passwords gratuitos como o **Lastpass** podem simplificar muito a sua vida, gerando uma password complexa diferente para cada sistema que utiliza, ao mesmo tempo que guardam as passwords em segurança e automatizam o seu login.
Autenticação de dois fatores ou autenticação multifator	A autenticação multifator, com mensagens de texto, dados biométricos ou códigos PIN gerados para si, irá protegê-lo se a sua password for roubada. Há muitas versões gratuitas (como o Google Authenticator, por exemplo) que podem ser usadas.

claranet cyber security

Use a VPN	As **VPNs** protegem a sua privacidade online e garantem que as suas comunicações empresariais são seguras. Evitam que os atacantes leiam o seu tráfego ao encriptar os dados.
Mantenha os seus sistemas sem *bugs*	Isto é fundamental. O patching deve ser realizado para reduzir o risco de que um malware explore uma vulnerabilidade com possíveis efeitos devastadores em toda a organização.
Use sempre *backups*	O que aconteceria se perdesse os seus dados? As causas podem ser várias, desde falha de hardware, as aplicações deixarem de funcionar ou roubo do dispositivo. Os utilizadores do **Office365**, ou de outras aplicações de produtividade na nuvem, devem criar sempre na nuvem. O back-up fica logo automaticamente na nuvem, estando a recuperação em caso de catástrofe integrada. Se for um utilizador do Onedrive ou do Google Drive, guarde o documento na sua pasta local para ter a certeza de que também fica guardado na nuvem (é preciso estar ligado à internet para isto funcionar).
Vigilância de *e-mails* de *phishing* e *websites* perigosos	Os atacantes usam *e-mail*s de **phishing**, mensagens de texto, mensagens de voz e outros métodos para o enganar. É importante que os utilizadores prestem atenção a todas as comunicações. Aqui estão algumas táticas simples: • Verifique o endereço do remetente. • Passe o rato sobre um *link* para ver um URL. Se parecer suspeito, é porque provavelmente o é. • Em caso de dúvida, navegue até ao *website* manualmente, usando o seu próprio favorito ou escrevendo o endereço para fazer o *login*, em vez de usar o *link* dentro do e-mail. • **NÃO CLIQUE** em anexos de pessoas que não confia. Uma boa ideia é usar um método alternativo de comunicação para falar com o remetente. Procure um número de telefone, endereço de email ou *chat online* fora dos limites do e-mail suspeito.
Seja um especialista em Wi-Fi	A maioria dos utilizadores domésticos não altera a *password* do router *Wi-Fi* e não sabe como os atualizar para o *firmware* mais recente. Para resolver esta questão, ative o WPA2/3 como padrão e verifique as suas *passwords* de administrador e as configurações de atualização automática. Escolha uma *password* comprida com mais de 15 carateres e registe a mesma no seu gestor de *passwords*.

claranet cyber security

Shadow IT	Tenha cuidado com os dados que guarda ou partilha. Se os guardar num serviço de nuvem, certifique-se de que este está autorizado para ser usado e de que você não está a desrespeitar nenhuma legislação de proteção e segredo dos dados ao usar ferramentas como o DropBox.
Speak up	A maioria das pessoas sente-se envergonhada quando é vítima de uma violação de dados. Contudo, se isso acontecer, é importante estar aberto e comunicar o quanto antes. Se reparou em algo estranho, diga ao seu empregador para que se possa agir com rapidez.

Esperamos que estes passos simples o ajudem a adaptar-se a estes tempos sem precedentes.

Stay safe!

A equipa da Claranet Cyber Security

claranet cyber security

Visite: claranet.pt/cyber-intelligence