NEWSLETTER

Segurança de Informação
e Continuidade de Negócio

MILLENNIUM BIM. AQUI CONSIGO.

Millennium bim

1ª Edição/ Junho/ 2017

Passwords ou Palavras-chave

As *passwords* fazem parte do nosso quotidiano, para aceder a *e-mails*, serviços bancários *on-line*, para a aquisição de bens ou para aceder aos dispositivos móveis (*smartphone*, *tablet*, *Laptop*, etc). Contudo, as *passwords* constituem também uma fragilidade, porque se alguém as descobre poderá roubar ou personificar identidade alheia, efectuando transacções financeiras ou acedendo á informações pessoais e/ou confidenciais de terceiros.

▪ Frases secretas

O desafio que todos nós enfrentamos é que os atacantes cibernéticos desenvolvem todos os dias métodos sofisticados para descobrir as nossas *passwords*, como por exemplo via ataques de "força bruta" (que consistem na verificação sistemática de todos os possíveis nomes de utilizadores e as respectivas *passwords* até que os correctos sejam encontrados), e eles estão constantemente aprimorando o que fazem. Isto significa que eles podem comprometer as *passwords* se as mesmas forem fracas ou fáceis de descobrir. Um critério importante para a protecção é o uso de *passwords* fortes. Quanto mais caracteres a *password* tiver, mais forte ela é e mais difícil será para um atacante quebrá-la. Entretanto, *passwords* longas e complexas podem ser difíceis de memorizar. Então, em paralelo, recomenda-se o uso de frases secretas, que são frases simples ou expressões fáceis de memorizar, mas difíceis de descobrir. Eis um exemplo: "Fazer-Dinheiro 24:7".

O que torna esta frase de acesso tão forte, aparte da mesma ser longa, é também o uso de letras minúsculas e maiúsculas, números e símbolos (lembre-se que espaços e pontuação são símbolos). Pode-se tornar a *password* ainda mais forte se trocar-se as letras por números e símbolos, como substituir a letra 'a' pelo símbolo "@" ou a letra "o" pelo número zero. Se um *site* ou programa limita a quantidade de caracteres que se possa usar para uma *password*, convém que se utilize o número máximo de caracteres permitidos.

▪ Uso seguro das frases secretas

Deve-se proteger as Frases Secretas. Não será de grande valia o uso da Frase Secreta se os criminosos puderem roubá-la ou copiá-la facilmente. Pelo que:

1. Certifique-se de usar uma Frase Secreta diferente para cada conta ou dispositivo que possua. Por exemplo, nunca use a Frase Secreta do seu trabalho ou conta bancária nas suas contas pessoais, como o *Facebook*, *YouTube* ou *Twitter*. Dessa forma, se uma das contas for invadida, as remanescentes ainda estarão seguras.

2. Nunca compartilhe uma Frase Secreta ou a sua estratégia de criação de Frases Secretas com outra pessoa, incluindo colegas de trabalho. Lembre-se, uma Frase Secreta é um segredo; se alguém sabe a sua Frase Secreta, ela não é mais segura.

3. Evite o uso de computadores públicos, como os que estão alocados em cafés, hotéis e/ou bibliotecas, para fazer o *login* numa conta de trabalho ou de um banco. Como qualquer pessoa pode usar esses computadores, eles podem estar infectados com algum código malicioso que captura todas as teclas digitadas, como um "*keylloger*". Apenas faça o *login* para a sua conta de trabalho ou contas bancárias em computadores ou dispositivos móveis confiáveis;

4. Tenha cuidado nos *sites* que exigem que se responda a perguntas pessoais. Estas perguntas são usadas em caso de esquecimento da *password* e da necessidade de redefini-la. Entretanto, as respostas a estas perguntas provavelmente poderão ser encontradas em outros *sites* na Internet, ou até mesmo na sua página do *Facebook*. Certifique-se de responder às perguntas pessoais apenas com informações que não estejam disponíveis publicamente ou informações fictícias que tenha inventado.

5. Muitas contas *on-line* disponibilizam uma autenticação de dois factores, também conhecida como a verificação em duas etapas. O que significa que para fazer o *login* (autenticação), em adição ao fornecimento da Frase Secreta, pode-se a título de exemplo, digitar-se um código secreto enviado ao seu dispositivo móvel. Esta opção revela-se mais segura comparativamente ao uso apenas da Frase Secreta.

6. Geralmente, os dispositivos móveis são configurados por forma a exigir um PIN para acedê-los. Lembre-se que um PIN não é nada mais que uma outra *password*. Quantos mais dígitos tiver o PIN, mais seguro ele será. Muitos dispositivos móveis permitem a mudança do número do PIN para uma Frase Secreta ou uso de impressões digitais, pelo que prefira estas em detrimento do uso do PIN.

7. Caso já não esteja a usar uma conta, não se esqueça de fechá-la, excluí-la ou desactivá-la.

8. Recomenda-se, viva e impreterivelmente, que não partilhe as *passwords* com terceiros, não deixe o seu posto de trabalho desbloqueado e não permita que terceiros usem o seu posto de trabalho na sua ausência; pois em caso de fraude efectuada por terceiros num determinado posto de trabalho, a responsabilidade será atribuída ao utilizador que estava *logado*.

Sabias que?

Eventos não previstos podem interromper as actividades e comprometer o desempenho, crescimento e até mesmo sobrevivência de uma organização. Pelo que, é de vital importância asseverar que as operações retomem o seu curso normal e previamente definido em caso de quaisquer incidentes. Assim, a **Continuidade de Negócio** é uma **ferramenta essencial**, que em colaboração com outras equipas/departamentos, propõe-se em assegurar que os objectivos definidos sejam atingidos mesmo quando a organização é exposta a algum **evento transitório ou disruptivo que possa interromper as suas operações de negócio**, como o **ataque *Ransonware WannaCry*** que decorreu numa escala global no pretérito dia 12 de Maio. O Grupo bim por estar ciente do exposto, possui uma Unidade de Continuidade de Negócio que visa acautelar eventos do género e salvaguardar os interesses dos seus Clientes, Colaboradores e do Grupo em si, sustentada nos procedimentos e políticas afins emanadas pelo Grupo Millennium, pelo Banco de Moçambique e pelo padrão internacional ISO 22301 (Gestão da Continuidade de Negócio).

www.millenniumbim.co.mz