PMI - (PROGRAMME DE MAÎTRISE DE L'INFORMATION)

REGRAS PARA CONSTRUIR PALAVRAS PASSE

INDICE

Introdução :

A palavra passe é o garante da segurança de dados quer seja no ambiente profissional (intranet Renault) ou na Internet.

Existem muitos utilizadores que desconhecem ou ignoram a importância de conhecer bem as regras de protecção da palavra passe e em consequência disso são alvos de acessos ilícitos ás suas contas .

01

As técnicas dos piratas informáticos

As técnicas dos piratas:

Os piratas informáticos possuem « dicionários « que contem as palavras passe mais frequentemente utilizadas.
Logo têm ao seu dispor meios para penetrar qualquer sistema de informação .

É por este motivo que deve ter o seguinte em conta a NÂO UTILIZAR , quando cria uma nova palavra passe :

- **o nome dum animal de estimação**
- **o nome de esposa ou filho.**
- **o nome da empresa onde trabalha**
- **o nome duma equipa de futebol**
- **o nome duma personalidade famosa (actor /cantor / jogador ..)**
- **o nome dum lugar ou pais**
- **uma palavra comun em linguagens diferentes .**

As técnicas dos piratas: ataques diretos

Tambem não convem utilizar os seguintes exemplos de palavras passe :

- datas de aniversários (anos / casamentos …)
- o numero de identificação do pc
- numero fiscal / s.social
- numero telefone

Embora possa parecer que este exemplos sejam dificeis de adivinhar podem já ser bem conhecidos no caso de frequentar as redes sociais (Facebook ,..,)

Os piratas têm outro método de obter palavras passe atravez de ataques diretos utilizando metodos de combinação alfanumerica para tentativas de acesso até acertarem no palavra passe correcta e acederem ao sistema de informação alvo do ataque.

Embora possa parecer um método obsoleto , com as velocidades dos pc's de hoje é bastante utilizado.

Assim sendo os tempos médios para « adivinhar « uma palavra passe são as seguintes :

Longueur	Minuscules	Minuscules + majuscules	Minuscules + majuscules + chiffres	Minuscules + majuscules + chiffres + caractères spéciaux
3	< 1 S	< 1 S	< 1 S	< 1 S
4	< 1 S	< 1 S	< 1 S	< 1 S
5	<1 S	<1 S	2.29 s	17.39 s
6	1.5 s	49.42 s	2.37 Mn	26.96 Mn
7	20.08 s	42.84 Mn	2.45 H	1.74 Jours
8	8.7 Mn	1.55 Jours	6.31 Jours	161.92 Jours
9	3.77 Heurs	80.44 Jours	1.07 Années	41.23 Années
10	4.1 Jours	11.46 Années	66.5 Années	3834.2 Années
15	132,964 Années	4.34 million d'années	60.9 billion d'années	26.67 trillion d'années
20	1.57 trillion d'années	1.65 quadrillion d'années*	55.8 quintillion d'années**	Une très grande durée

*1,655,435,220,000,000 Années

**55,805,770,300,000,000,000 Années

A reter : quanto maior e combinada for a palavra passe mais tempo demora que seja decifrada.

02

Boas práticas

Boas praticas – como manter uma palavra passe sólida .

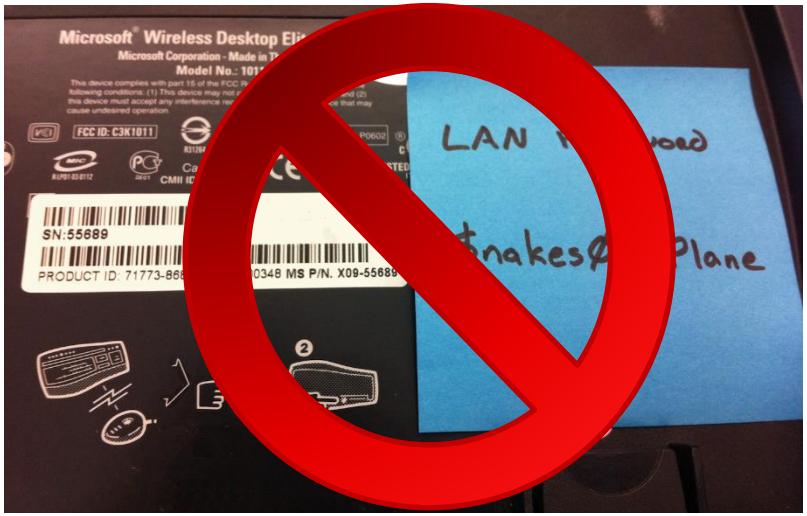
As regras da Renault :

- Palavra passe composto por 6-8 caracteres (alfa+numerico)
- Deve ser diferente do seu IPN .
- Os três primeiros caracteres não devem ser idênticos
- Os três primeiros caracteres não devem ter a ordem coincidente com o IPN
- Não reutilizar um das últimas seis palavras passe
- Deve substituir 2 caracteres no minimo quando muda a palavra passe

Boas praticas – como deve guardar a palavra passe.

Recomendações :

- nunca guardar as suas palavras passe em locais acessiveis por outras pessoas (ficheiros em redes partilhadas , post-its , parte tras do teclado ……)



Boas praticas – acessos internet : não utilizar a mesma palavra passe para sitios diferentes .

Em média , um utilizador está associado a uma vintena de sites internet que necessitam de autenticação via palavra passe.
A maioria dos utilizadores utilizam a mesma palavra passe para todos os sites.

Esta prática é perigosa dado que basta haver um site que seja atacado com sucesso por um pirata informático e as restantes ficam imediatamente em risco . O pirata pode assim obter dados de todos os restantes sites usando e mesma palavra passe .
Tal como aconteceu com o site da LINKEDIN em 2012 em que num ataque pirata foram furtados 6,5 milhões de palavras passe , colocando os dados de todos os utilizadores em perigo relativamente a outros sites .

A reter :

- nunca se deve utilizar a mesma palavra passe para acessos em sitios diferentes.

Boas praticas – o que fazer no caso da minha palavra passe ser comprometida

Deve imediatamente :

- mudá-lo para evitar que possa ser reutilizada por outra pessoa.
- informar o serviço de segurança para que tomem as ações necessárias

.

Resumindo devemos tratar as palavras passe como tratamos a roupa interior

Devem ser trocados frequentemente

Nunca partilhar com ninguem

Devem ser guardados em lugar proprio

Quanto maiores , melhor !

03

Truques e dicas

Truques e dicas – Gestão de palavras passe

É impossível de se lembrar de todas as palavras passe das contas que possa ter . Uma solução consiste em classificar os diferentes acessos que tem em função da criticidade e aplicar a regra seguinte :

1) Sites não sensíveis (tempo , receitas cozinha …) : usar a mesma palavra passe em todos os sites

2) Sites ligeiramente sensíveis (redes sociais …) : usar a mesma palavra passe para todos os sites mas que seja diferente da que utilizada em sites não sensíveis .

3) Sites sensíveis (bancos , financas,….) utilizar uma palavra passe robusta e diferente para cada site .

Obter uma palavra passe robusta pode parecer complicado . Para vos ajudar devem utilizar o sistema de « frase > passe « :

1) Por exemplo escolher a seguinte frase : **A**manhã **v**ou **c**omprar **c**roissants **p**ara **o** **p**equeno **a**lmoço.

2) A seguir retira as letras iniciais de cada palavra : Avccpopa

3) A seguir acrescenta o dia correspondente a amanhã como prefixo e o mes como sufixo,

E obtemos a seguinte palavra passe :

18Avccpopa02