ZURICH

Computadores portáteis
Prevenção de perdas

Computadores portáteis
Prevenção de perdas

Os computadores portáteis (notebooks / laptops / tablets) tornaram-se um dos mais populares itens entre os oportunistas e ladrões.

Neste informativo técnico, você encontrará algumas recomendações, que embora não esgotem o assunto, proporcionam algumas ideias de como implementar e manter uma boa estratégia de segurança.

A educação dos usuários é essencial para minimizar perdas.

As regras principais são:

- Não fique desatento ao seu *notebook*!
- Evite carregá-lo por toda parte, leve-o apenas quando for utiliza-lo.
- Acondicione o *notebook* em mochilas ou valises comuns, descaracterizando o seu conteúdo.

NAS RUAS:

NÃO USE O *NOTEBOOK* EM QUALQUER LUGAR!

- Evite parar próximo ao meio fio enquanto espera para atravessar a rua. É nessa hora que age a maioria dos assaltantes, principalmente os com motocicletas;
- Não leve seu *notebook* nas mãos, sempre utilize bolsas ou mochilas e as segure firmemente.

NO CARRO:

- Nunca deixe o *notebook* dentro do carro, nem mesmo no porta-malas, quando não estiver presente;
- Nunca deixe o *notebook* à vista, mesmo que você esteja no carro;
- Enquanto dirige, posicione a maleta do *notebook* entre o assento do motorista e o banco traseiro, ou no porta-malas.

SEGURANÇA EM VIAGENS: AEROPORTOS, ESTAÇÕES FERROVIÁRIAS...

- Nunca deixe o equipamento sem supervisão;
- Nunca despache um *notebook* como bagagem;
- Enquanto o *notebook* passa pelo raio-X, não o perca de vista;
- Se o agente de segurança solicitar verificação, você é que deve manuseá-lo;
- Nunca permita que outros toquem no computador.
- Quem quer que se sente atrás ou ao seu lado pode ver a tela de seu *notebook*, logo proteja suas informações e sua privacidade;

FILTROS DE PRIVACIDADE:

- Filtros de tela, de tecnologia especial, permitem que a tela do *notebook* seja visível apenas por aquele que esteja diretamente à sua frente. Outras pessoas, posicionadas em ângulos, diferentes vêm uma tela escura.

ANTES DE VIAJAR:

- Faça, sempre, backup de seus arquivos antes de viajar com seu *notebook*;
- Se não se pode evitar a perda financeira decorrente de um eventual roubo, com certeza pode-se evitar a perda de dados e informações.

SEGURANÇA EM VIAGENS: NOS ÔNIBUS, TRENS, AVIÕES...

- Não confie no fato de estar em uma aeronave ou ônibus, um espaço pequeno e com muitas testemunhas, achando que, por isso, tem menores chances de ser roubado;
- Quando você não estiver usando seu *notebook*, coloque-o debaixo do assento à sua frente, em vez de deixá-lo no bagageiro superior, facilmente acessível por estranhos.

TRAVAMENTO COM CABOS E CADEADOS

- Use uma trava de segurança para fixar o *notebook* as escrivaninhas, mesas, armários, etc.
- Use uma trava de segurança... Inclusive em hotéis.

NO ESCRITÓRIO

- Se a sua mesa de trabalho fica numa área de grande tráfego de pessoas, acessível ao público, bloqueie o acesso ao seu *notebook* toda vez que se ausentar de sua mesa;
- Não posicione *notebooks* próximos às janelas externas, onde eles estejam sujeitos a furto;
- Não deixe *notebooks* sem supervisão em mesas de trabalho, especialmente de um dia para o outro.

EM APRESENTAÇÕES, *WORKSHOPS* E SEMINÁRIOS

- Mantenha o *notebook* sempre consigo;
- Durante intervalos (*coffee breaks*, almoço, etc.), solicite aos organizadores do evento que tranque a sala ou para guardá-lo em armários de segurança, com controle e supervisão contínua.

MEMÓRIAS PORTÁTEIS (USB)

Mais conhecidos como Pen Drives são pequenas unidades de memória que se conectam ao computador por intermédio de uma porta USB, facilitando o transporte de dados. Suas principais vantagens são o tamanho reduzido, facilidade de instalação e transporte com menor risco de danos físicos.

Cuidado: Se você estiver desatento, seus dados podem ser facilmente copiados com uso de pen drivers.

SOFTWARES E PROCEDIMENTOS DE SEGURANÇA

- Programas de segurança protegem, preservam e asseguram dados e informações proprietárias;
- Deixe ativado o bloqueio de tela automático, no melhor intervalo que lhe seja conveniente, sempre solicitando a senha para desbloqueio;
- Use programas de Backups para fazer cópias de segurança frequentes de seus arquivos importantes;
- Use programa de criptografia de disco;
- Use um antivírus confiável.

CONTROLES DE GERENCIAMENTO

- Mantenha inventários de equipamentos sempre atualizados, constando sempre os dados de seu equipamento: modelo, número de série, resposável;
- Certifique-se de gravar o código de suas chaves de travas antifurto. Isto vai poupar-lhe dos inconvenientes, caso tenha que repor as chaves;
- Grave o nome e contato da empresa em todos os *notebooks*;

TREINAMENTO DOS USUÁRIOS DE *NOTEBOOKS*

Proporcione aos usuários, treinamentos anuais de prevenção e lembretes periódicos para manter a consciência de segurança. Políticas e Procedimentos devem cobrir itens como:

- Os usuários devem ser responsáveis pela proteção e segurança do equipamento atribuído;
- Os usuários devem ser responsabilizados na eventualidade de perda do equipamento negligenciado;
- Requeira a assinatura dos usuários na cópia da política de segurança;
- Audite anualmente políticas, procedimentos, equipamentos designados e relações de “softwares” instalados.
- Investigações de perdas devem ser feitas em todos os casos de roubo/ furto.
- Não aceite facilmente perdas, danos ou furtos de computadores portáteis.
- Investigue todas as ocorrências!

Zurich Brasil Seguros
Av. Jornalista Roberto Marinho, 85 - 23º andar
Brooklin Novo – 04576-010
São Paulo, SP – Brasil

Publicação do Departamento de Risk Engineering da Zurich Brasil Seguros S.A.
Edição Digital nº 01 - Atualizada em Dezembro/2020
Para receber outros informativos ou obter maiores informações, contatar o Departamento de Risk Engineering da Zurich.
E-mail: engenharia.riscos@br.zurich.com

ZURICH®