

MANUAL DE CONDUTAS SEGURAS

**1ª edição
Agosto 2015**



ASSOCIAÇÃO DOS AGENTES DE SEGURANÇA DO
PODER JUDICIÁRIO DO ESTADO DE SÃO PAULO

Índice

Apresentação 03

Delitos comuns 04

Estatísticas de combate a delitos 05

Características básicas da agressão 06

Prevenção em estacionamentos 07

Prevenção na condução de veículos 10

Prevenção em semáforos 10

Prevenção contra abordagem de veículos 12

Prevenção em Caixas Eletrônicas 13

Prevenção na rua 14

Prevenção em redes sociais 16

Prevenção na Internet 18

Engenharia social 22

Considerações finais 23

Apresentação.

Este manual é um esforço dos Agentes de Segurança Judiciários desenvolvido com a ajuda de especialistas em segurança e prevenção contra a violência urbana. Busca colaborar na elaboração de condutas seguras e simples a serem aplicadas no dia a dia para promover a cultura de segurança.

Devido aos limites do presente trabalho, demos prioridade nesta primeira edição ao cenário de múltiplos riscos e de motivação patrimonial; procuramos apresentar regras básicas de prevenção para mitigar riscos e diminuir as oportunidades a serem aproveitadas por agentes agressores.

As recentes e sofisticadas formas de atuação do crime organizado serão objeto de edições futuras dedicadas ao estudo específico das estruturas com crescente potencial ofensivo e suas diversas demonstrações de ousadia em perpetrar ações criminosas contra autoridades, agentes e patrimônio público.

Cuidamos também de analisar a exposição constante de autoridades e de funcionários deste Tribunal na imprensa e em diversas mídias sociais que acabam por revelar rotinas e hábitos.

O esforço dos Agentes de Segurança Judiciários conjuntamente com outras iniciativas de formação e capacitação promovidas por nossa associação – ASPoJESP, está a serviço da construção de possibilidades de solução e à disposição dos demais protagonistas da instituição.

Para efeitos deste manual, utilizaremos a palavra **ASSALTO** em sua acepção militar e como sinônimo de **ataque surpresa, ação ou efeito de surpreender; tomar de assalto**. Sendo assim, o termo assalto significa surpreender e dominar a vítima. Com a vítima em poder do agressor, as ações seguintes podem evoluir para o roubo, sequestro, lesão corporal, homicídio e demais condutas criminosas.

I - Delitos Comuns

De acordo com dados de Segurança Pública dos Vários Estados da Federação, as modalidades de delitos mais frequentes nos centros urbanos são:

1 - SEQUESTRO RELÂMPAGO (Oportunista).

Possui a característica de ocorrer com duração de 1 a 24 horas. É o tipo de delito que visa à realização de saques e de transações bancárias.

2 – SEQUESTRO COM PEDIDO DE RESGATE (Planejado).

A seleção da vítima, para este tipo de delito, é feita geralmente pelo tipo de carro, pelo status do cidadão, por seu nível hierárquico.

3 – FURTO e ROUBO A RESIDÊNCIA (Oportunista e Planejado).

Geralmente o agente agressor se utiliza dos movimentos de entrada e saída do morador. Tais movimentos constituem pontos de maior vulnerabilidade.

4 – ROUBO A MÃO ARMADA (Oportunista e Planejado).

O resultado de roubo a mão armada (em que o agente agressor surpreende a vítima) depende muito da reação da vítima. O delinquente age de acordo com o nível de ameaça que a vítima pode representar.

II - Estatística de Combate a Delitos

95 % PREVENÇÃO

02 % REAÇÃO

03 % ACASO

Não existe garantia de 100% de segurança. Dados e pesquisas demonstram, no entanto, que a ação preventiva é a melhor solução em todos os casos.

III – Fases Pré Delitos

1- PRÉ-ELEIÇÃO DO ALVO - Essa fase pode levar meses, dias ou apenas alguns segundos. É a fase em que o agente agressor seleciona o alvo a ser abordado.

2 - IDENTIFICAÇÃO DO ALVO - O alvo foi escolhido. Geralmente o mais distraído, mais fraco ou apenas aquela vítima que possui algo que o agente agressor procura (foco da investida).

3 - VIGILÂNCIA - É o período em que o agressor avalia toda a situação antes do ataque (monitoramento) e reúne informações.

4 - PLANEJAMENTO - O delinquente já possui todas as informações de que precisa; agora ele planeja como será o ataque (dia, hora, forma de abordagem, arma etc.).

5 - ATAQUE - O agressor faz a abordagem. Nesta fase já não há como fazer prevenção. Os percentuais de êxito em ações de interrupção são menores do que 5%.

IV – Características Básicas da Agressão

Quando um agressor realiza o assalto é porque falharam as prevenções mínimas e significa que:

A vítima assumiu uma posição vulnerável e diminuiu a exposição do agente agressor. A vítima demonstrou a possibilidade de estar em posse de valores e foi selecionada. A vítima não percebeu a aproximação do estranho. Foi abordado de forma surpreendente!

1 – O agressor não quer ser exposto.

Evite se posicionar de forma isolada, em locais de pouca visibilidade, sem rotas de fuga, com mãos ocupadas e de costas para o exterior (ex. procurar a chave na bolsa de frente para o veículo ou porta e de costas para a rua ou multidão).

2 – O agressor sempre seleciona a vítima.

Não seja uma vítima atraente. Considere o trajeto de deslocamento. Planeje e classifique os riscos do local onde permanecerá; selecione roupas e acessórios que evitem o destaque financeiro.

3 – O agressor escolherá a vítima mais fácil, ou seja, a mais distraída, fraca, despreparada.

Evite dividir a atenção com aparelhos eletrônicos nos deslocamentos. Crie um círculo de atenção a sua volta, exercite a percepção sobre quem se aproxima, esconda uma das mãos e caminhe com decisão e passos firmes. Durante o assalto, o agressor está nervoso e com medo.

Demonstre calma e não reação.

A vítima surpreendida no assalto tem apenas **5% de chances de êxito**. Neste cenário, só resta reduzir os danos protegendo a própria vida e a dos mais próximos evitando:

Movimentos bruscos;

Diálogos que busquem convencer o agressor a desistir do crime;

Posicionar-se entre o agressor e sua rota de fuga.

Reagir é uma atitude de altíssimo risco.

A prevenção se completa observando atitudes suspeitas, como trajas em desacordo com as condições climáticas, comportamentos que ocultem as mãos, o olhar fixo, ou seja, atenção à linguagem corporal das pessoas.

ERRADO acreditar que nunca seremos vítimas.

CORRETO adotar atitudes preventivas evitando ser a vítima perfeita para a abordagem delituosa.

V - Prevenção em Estacionamentos

Antes de sair, devemos planejar o trajeto do deslocamento, o local que iremos frequentar, o estacionamento do veículo e o retorno.

Muitas vezes, quando chegamos, encontramos o local iluminado e a rua movimentada. Ao retornarmos, dependendo do horário, a rua poderá estar deserta e escura.

Considerando o princípio da prevenção descrita acima, ao buscarnosso veículo em local isolado e pouco iluminado estaremos desrespeitando as duas primeiras regras, ou seja, estaremos em um local que não expõe o agressor e teremos algo a oferecer (o veículo e demais pertences). Se ainda agregarmos o elemento da atenção (nos posicionar de costas para a rua enquanto procuramos as chaves ou **não manter a efetiva atenção às áreas próximas**) seremos a vítima perfeita a ser tomada de assalto.

Ao retornar para o veículo, reavalie a situação, caso desconfie de algo ou de alguém, passe direto por seu veículo. Não deixe que percebam que o veículo é de sua propriedade.

Sempre tire a chave da ignição de seu carro, não o deixe ligado, mesmo quando for apenas para abrir o portão e entrar na garagem.

Não deixe a chave de casa no veículo, pois, nesse caso, um assalto ao veículo pode evoluir para um assalto à residência ou até mesmo um sequestro.





Veículo parado na rua aumenta o grau de vulnerabilidade e, por si só, é alvo atraente. Devemos optar por estacionamentos vigiados sempre que possível (ou estacionamentos pagos).

Não fique dentro do carro estacionado. Dentro de um carro parado na rua sempre existe uma vítima perfeita.

Não utilize celular, conte dinheiro ou manuseie documentos e demais pertences dentro de um carro estacionado.

Não permita que objetos atraentes ao agressor permaneçam na linha de visão. Bolsas, relógios, óculos e demais pertences devem ficar abrigados.

O agressor elege sua vítima dentre as que ofereçam maior facilidade em obter benefício.

VI - Prevenção na Condução de Veículos

IDENTIFICAÇÃO → Evite colocar adesivos nos vidros. Eles podem revelar seus hábitos (condomínio, academia, quantidade de filhos etc.) e facilitar a localização de seu veículo.

PORTAS E VIDROS → Mantenha as portas sempre travadas e vidros fechados. Se possível, instale películas do tipo insulfilm.

OCORRÊNCIAS PREVISÍVEIS → Fique atento e desconfie de batidinhas na traseira do seu veículo, pneu furado em lugares ermos, líquido no para-brisas ou pedras. Objetos na via bloqueando ou restringindo o fluxo de veículos. Pedido de ajuda/socorro.

CUIDADO! PARADOS, SOMOS ALVO FÁCIL!

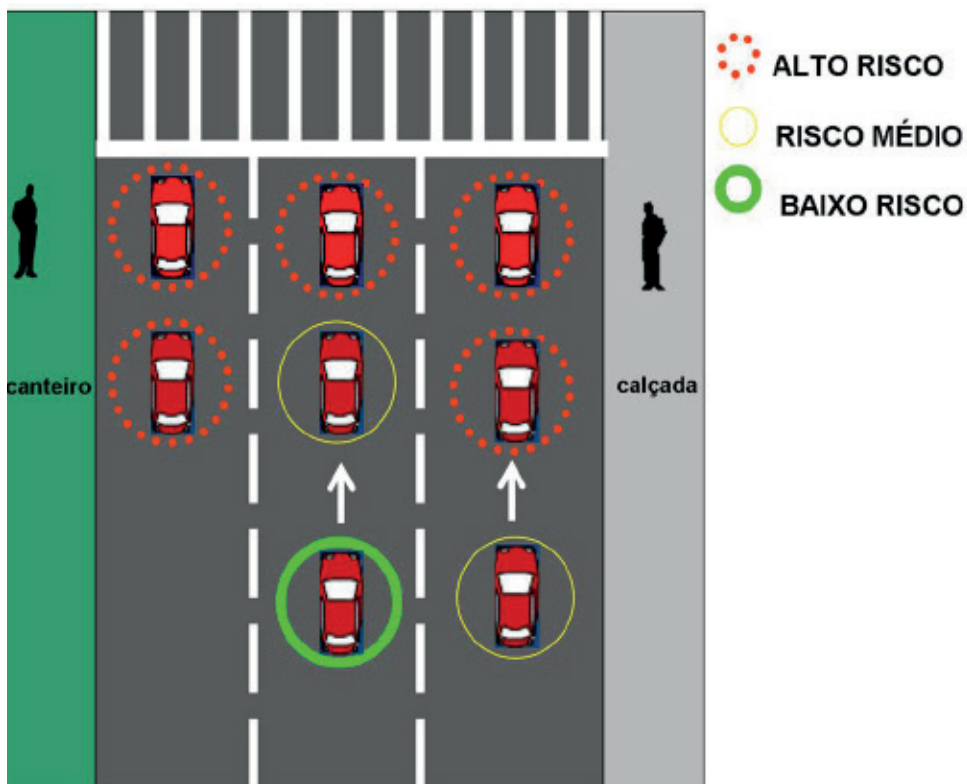
VII - Prevenção em Semáforos

Ao avistar um semáforo, devemos reduzir a velocidade e tentar chegar ao sinal quando este estiver verde. Dessa forma o veículo sempre estará em movimento evitando paradas e exposições;

Devemos manter distância segura do veículo a nossa frente (o necessário para manobra de evasão). Tal distância constitui elemento inibidor à abordagem, pois garante margem de manobra para continuar em movimento, além de demonstrar atenção. Sendo assim, o agente agressor tende a selecionar a vítima mais dispersa e eleger o veículo que estiver preso entre os carros.

Quando não for possível evitar o sinal fechado devemos ficar afastados da calçada, de preferência utilizando a faixa central. O assalto tende a ocorrer pelas calçadas, principalmente pelo lado do condutor, situação em que o agente agressor tem acesso e domina a vítima.

Observe a figura sobre zonas de riscos abaixo:



VIII - Prevenção Contra Abordagem de Veículos

Se for abordado, proceda da seguinte forma:

1- TENHA E PEÇA CALMA:

Mantenha-se calmo e peça que o agressor tenha calma, faça-o se sentir no controle da situação. Agressores acuados ou com medo podem agir por impulso.

2- OBEDEÇA RAPIDAMENTE:

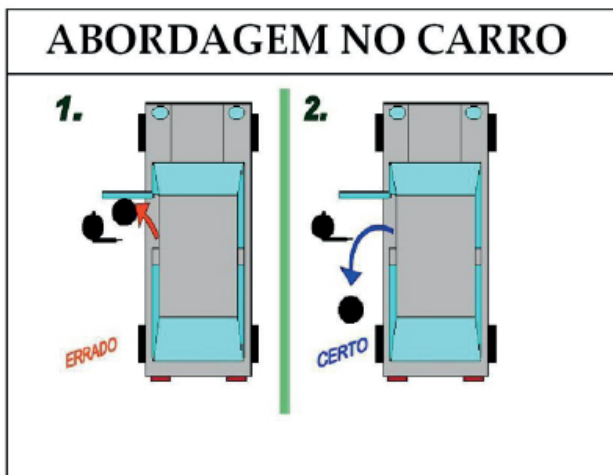
Obedeça às ordens do assaltante e fique calmo, porém com rapidez.

3- INFORME O QUE VAI FAZER:

Mantenha as mãos onde o assaltante possa vê-las (no volante). Se for pegar objetos, soltar o cinto ou abrir a porta informe o assaltante e faça movimentos suaves. Lembre-se que o assaltante está nervoso.

4- Se descer do carro, faça de maneira a NÃO OBSTRUIR ou DESAFIAR o assaltante.

Observe a ilustração a seguir:



No Ponto 1, ao sair pela frente do carro, constituímos um obstáculo para o assaltante. Além disso, o assaltante pode interpretar o seu movimento como uma investida contra ele. Neste caso, a vítima será, certamente, ferida ou agredida.

No Ponto 2, ao sairmos, devemos nos deslocar para a parte traseira do veículo, o assaltante terá certeza de que queremos ir embora sem resistência.

IX - Prevenção em Caixas Eletrônicos

Devemos Sempre aplicar as três Regras Básicas de Prevenção:

1 – Exposição (o agressor não quer se expor e prefere locais com baixa luminosidade e pouca movimentação);

2 – Seleção (o agressor sempre elege a vítima que lhe proporcione auferir vantagem ou menor resistência);

3 – Atenção (o agressor sempre seleciona a vítima mais distraída e dispersa e que permite a aproximação).

REGRA: NUNCA devemos utilizar caixas eletrônicos no período noturno. É comum que pessoas, nesse horário, realizem saques.

MELHORES CAIXAS → Em mercados, shoppings ou outros locais onde há luminosidade, seguranças e grande número de pessoas;

CAIXAS INSEGUROS → Locais com pouca movimentação, pouca luminosidade, isolados e caixas com exposição pública da retirada do dinheiro;

CÂMERAS DE SEGURANÇA → Elas não impedem que alguém o roube;

PARTES DOS CAIXAS → Verifique e force as partes dos caixas, agentes criminosos tentam substituir e até mesmo sobrepor peças para cópia de cartões, identificação de senhas e impedimento da saída de dinheiro.

Nunca Aceite Ajuda ou Permita Aproximação em Caixa Eletrônico!

X - Prevenção na Rua

AÇÃO DELITUOSA	REAÇÃO DA VÍTIMA
ALGUÉM EM ATITUDE SUSPEITA EM SUA DIREÇÃO	Considere um agente agressor, mude sua direção, volte mantendo o espaço entre ele e você.
ELE APERTOOU O PASSO EM SUA DIREÇÃO	Procure um local seguro, movimentado (Ex. Loja, mercado, shopping, empresa, etc...)
NÃO HÁ LOCAIS PARA SE PROTEGER	Corra e observe o comportamento do suspeito. Corra antes que ele feche o espaço entre vocês. Depois da abordagem jamais corra.
SE ELE CORRER EM SUA DIREÇÃO	Ele VAI cometer um delito, sendo assim GRITE . O agressor evita a exposição e tende a não correr atrás de você; ele não quer chamar a atenção. Nesta situação prefere escolher outra vítima menos preparada, mais distraída e menos atenta.

REGRA: Quando intuímos que alguém irá nos abordar, não devemos **nunca** fechar o espaço. É comum percebermos inconscientemente a expressão corporal. Muitas vítimas relatam que perceberam que algo iria acontecer e não agiram preventivamente.

O que **GRITAR** quando está sendo seguido ?

Não grite por socorro. Instintivamente as pessoas recuam procurando se afastar.

Grite "**fogo**" desperta o interesse das pessoas, fazendo-as sair das casas para ver onde está o fogo.

Gritar o nome de alguém, "**Paulo**", é a melhor opção, o agente agressor procura a vítima mais fácil e pode desistir da abordagem por acreditar haver mais pessoas no local (quem é Paulo, homem, policial?). As chances de o agressor desistir da abordagem aumentam.

Após a Abordagem na rua devemos:

- 1- Demonstrar calma;
- 2- Pedir calma;
- 3- Deixar que o agressor se sinta no controle da situação;
- 4- Não resistir; entregar todos os objetos que forem pedidos;
- 5- Não transmitir raiva ou sentimento de vingança;
- 6- Considerar que contra arma de fogo ou faca não existe força física suficiente;
- 7- Considerar que agressor sob efeito de álcool e drogas tem reflexos alterados, nesse caso devemos realizar movimentos calmos e suaves;
- 8- Não criar situações que retirem do agressor a sensação de controle;
- 9- Não revidar agressões físicas ou contra nossos acompanhantes;
- 10- Ao falhar a prevenção, falharam também 95% de chances de êxito. O objetivo principal é reduzir os danos, evitar agressões e **sobreviver** ao assalto.

XI - Prevenção em Redes Sociais



As redes sociais são um novo ambiente de convívio. Trazem consigo ameaças e riscos como qualquer outro ambiente de relações humanas, pois permitem aos usuários:

- Fornecer informações sobre si;
- Acessar informações sobre outros usuários;
- Utilizar mecanismos de comunicação e informações;
- Agrupar-se de acordo com afinidades, características interesses e objetivos em comum;
- Criar, gerenciar e compartilhar uma espécie de diário público com informações como: Quem somos. Onde estamos. Objetos de nosso interesse. Nossos conhecidos. Locais em que possivelmente estaremos. Nossas reflexões e relações afetivas e nossa capacidade econômica.

Atrativos e Possibilidades.

- Rápida velocidade de propagação de informações;
- Grande quantidade de usuários;
- Facilidade de acesso e possibilidade de anonimato;
- Grande quantidade de informações pessoais;
- Tempo em que as informações ficam disponíveis.

Principais Riscos.

- Invasão de privacidade;
- Furto de identidade;
- Invasão de perfil;
- Instalação de programas maliciosos;
- Contato com pessoas mal intencionadas;
- Disponibilização de informações para criminosos, podem ser usadas em tentativas de sequestro e furto de bens.
- Phishing, forma de fraude eletrônica, caracterizada por tentativas de adquirir fotos, músicas e outros dados pessoais fazendo-se passar por pessoa confiável ou por empresa enviando uma comunicação eletrônica oficial;
- Uso indevido de informações;
- Danos à imagem e à reputação;
- Vazamento de informações;
- Recebimento de mensagens contendo códigos maliciosos.

XII - Prevenção na Internet

Devemos lembrar dos sete pontos vulneráveis no ambiente on-line, segundo a empresa **CISCO SYSTEMS INC.**

- 1- Sex appeal (apelo sexual)
- 2- Ganância
- 3- Vaidade
- 4- Confiança
- 5- Preguiça
- 6- Compaixão
- 7- Urgência

Para Preservar Nossa Privacidade Devemos:

- Considerar que estamos em um local público;
- Refletir antes de divulgar (não há como controlar as dimensões que a divulgação tomará);
- Usar opções de privacidade oferecidas pelos sites, ser o mais restritivo possível;
- Manter perfil e dados privados;
- Restringir acesso ao endereço de e-mail;
- Ser seletivo ao aceitar contatos;
- Não acreditar em tudo o que lemos;
- Ser cuidadosos ao nos associar a grupos e a comunidades;
- Ser cuidadosos ao divulgar fotos e vídeos, observando onde foram gerados;
- Não divulgar planos de viagem ou tempo de ausência da residência;

- Ao usar redes sociais baseadas em geolocalização, somente fazer check in em locais movimentados, fazer check in ao sair do local e não quando chegar.

Devemos sempre respeitar a privacidade alheia

- Evitar falar sobre ações, hábitos e rotina de outras pessoas;
- Não divulgar sem autorização imagens em que outras pessoas apareçam, mensagens/imagens copiadas do perfil de usuários que restrinjam o acesso;
- Imaginar a reação das pessoas sobre o que tornamos público. Prevenir é ter atenção e evitar exposição. Nunca saberemos quem está do outro lado.

Proteção de E-mail

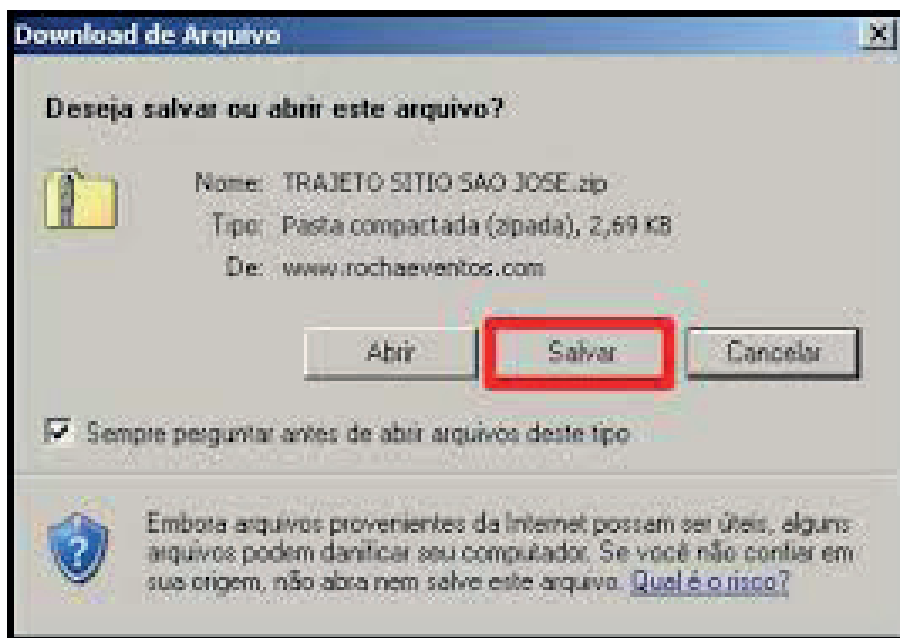
- Ao encaminhar mensagens devemos retirar o e-mail das pessoas que nos enviaram;
- Quando enviar e-mail para várias pessoas, onde a resposta não necessite ser de conhecimento de todos, devemos colocar todos os endereços em cópia oculta;
- Nunca devemos abrir anexos com extensões .exe ou suspeitos, só devemos abrir arquivos se tivermos certeza do conteúdo.

A curiosidade matou o gato.

- Nunca devemos clicar em links, se não tivermos certeza de que sejam confiáveis, eles podem estar mascarados - os hackers mascaram até mesmo o nome do e-mail do remetente;
- E-mails de redes conhecidas como SPAM visam arrecadar grande número de endereços eletrônicos, não devemos repassar esse tipo de e-mail.

•Devemos cuidar ao repassar dados pessoais em listas. Os dados podem ser utilizados por sequestradores, ladrões e chantagistas. Não devemos acreditar em tudo que está na internet. Reflexão, análise e observação. A internet é uma área pública que pode conter qualquer informação.

Preste muita atenção nesta tela!



Podemos Manter Nosso Computador Seguro com:

- Todos os programas instalados nas versões mais recentes e todas as atualizações aplicadas;
- A utilização e manutenção dos mecanismos de segurança como: antispam, antimalware, firewall pessoal, etc;
- Devemos desconfiar até das mensagens enviadas por conhecidos. Podem ter sido enviadas de contas falsas ou inválidas;

- Devemos suspeitar ao acessar links reduzidos e usar complementos que permitam expandir o link, antes de clicar sobre ele;
- Ser cuidadosos ao elaborar senhas e preferir as longas, compostas de diferentes tipos de caracteres. Não utilizar dados pessoais, como nome, sobrenome e datas. Usar senhas diferentes para diferentes acessos. Se possível, devemos evitar o uso de senha em computadores de terceiros;
- Habilitar as notificações de login;
- Lembrar sempre de fechar nossas sessões (logout);
- Denunciar aos responsáveis pela rede social abusos, tais como: imagens indevidas, perfis falsos, spam.

Para Proteger Menores e Incapazes

- Devemos orientar sobre os riscos no uso das redes sociais;
- Respeitar os limites de idade estipulados pelos sites;
- Deixar o computador em um local público da casa;
- Orientar para não se relacionar com estranhos, não marcar encontros e não usar a webcam;
- Orientar para não divulgar a localização geográfica (atual ou futura), dados pessoais e hábitos familiares;
- Verificar sempre as amizades e os assuntos;
- Passar noções e hábitos de segurança para toda família.

Para Proteger a Vida Profissional, devemos:

- Cuidar da imagem profissional
- Antes de divulgar, avaliar o risco e lembrar que a informação poderá ser acessada por pessoas do seu ambiente de trabalho e fora dele;

- Observar se ela não fere os preceitos previstos nas normas da instituição;
- Cuide do seu lixo, informações sigilosas e importantes devem ser destruídas antes de ser descartadas.

XIII - Engenharia Social

É a “garimpagem” de informações vitais sobre uma pessoa, produto ou organização como forma de análise e preparação de um ataque. Também considerada sinônimo de espionagem. Tais informações são provenientes quase sempre de pessoas próximas, cônjuges, pais, filhos e amigos.

Devemos:

- Evitar cadastro de dados pessoais em fontes desconhecidas ou inidôneas. Tais dados podem ser usados para a prática de crimes no sistema financeiro (abertura de contas bancárias, aquisições de cartões etc);
- Cuidar do conteúdo que publicamos nas redes sociais. Evitando opiniões ofensivas a pessoas, empresas ou instituições, pois tais opiniões podem ser enquadradas como criminosas.

Previna-se com regras simples no espaço cibernético.

- Devemos evitar postar fotos ou vídeos nas redes sociais, sobretudo de nossa família, bens (casa, carro etc) e o local onde residimos. Essas informações são monitoradas e podem facilitar ações ilícitas, colocando em risco nossa integridade e nossos familiares;
- Mesmo o ambiente privado dessas redes não garante confidencialidade, podendo inclusive comprometer nossas atividades profissionais;

• Não devemos usar senhas relacionadas ao conteúdo publicado nessas redes (preferências esportivas, religiosas, hobbies etc.) nem à vida privada (nome ou sobrenome de familiares ou de animais domésticos, placa do automóvel, data de nascimento, cidade onde reside, etc.). A partir dessas informações, os criminosos cibernéticos direcionam suas ferramentas e obtêm acesso a sistemas, contas de e-mail e outros. Devemos evitar palavras comuns de dicionários.

XIV - Considerações Finais

Valorizando a Vida.

1 - Nossa preocupação deve se voltar sempre à prevenção para evitar a surpresa (assalto). Ao assumirmos a postura preventiva estaremos construindo uma cultura de segurança;

2 - Ao relevar provocações no trânsito, em bares ou em boates estaremos nos prevenindo de resultados duvidosos. Isso é sinal de inteligência e não de covardia;

3 - Se cairmos vítimas de ataque surpresa, significa que perdemos 95% das chances de êxito em evitar danos, mas podemos reduzir suas extensões entregando os objetos de valor e colaborando para ficar o menor tempo possível sob domínio do agressor. Não há nada mais valioso que a vida;

4 - Devemos evitar toda e qualquer situação que nos exponha a riscos desnecessários.

Nossos agradecimentos especiais aos Agentes de Segurança Judiciária do TRT2 empenhados em promover a segurança institucional de todo Poder Judiciário e em colaborar com o desenvolvimento técnico dos servidores de diversos tribunais.

Mais informações:
www.aspojesp.com.br
aspojesp@gmail.com



ASSOCIAÇÃO DOS AGENTES DE SEGURANÇA DO
PODER JUDICIÁRIO DO ESTADO DE SÃO PAULO