Cartilha de Segurança na Internet

STi

SUPERINTENDÊNCIA DE
TECNOLOGIA DA INFORMAÇÃO

Índice

Dispositivos Móveis

O uso de tablets, smartphones e celulares está cada vez mais comum e inserido em nosso cotidiano, sempre tem alguém usando um dispositivo móvel, seja para tirar fotos, acessar e-mails, ler notícias ou comentar sobre o que está fazendo nas redes sociais. Porém, é importante estar ciente dos riscos que o uso de dispositivos móveis podem representar para que, assim, possa tomar os devidos cuidados.

Ao usar seu dispositivo móvel:

• Instale um programa antivírus, antes de instalar qualquer tipo de aplicativo;
• Mantenha-o seguro (com a versão mais recente de todos os programas instalados);
• Não siga links recebidos por meio de mensagens eletrônicas (SMS, e-mails, redes sociais, etc.);
• Desconfie de mensagens recebidas, mesmo que enviadas por conhecidos;
• Mantenha controle físico sobre o seu dispositivo (procure não deixá-lo sobre a mesa e cuidado com bolsos/bolsas quando estiver em ambientes públicos);
• Proteja suas senhas , não as deixe salvas em seu celular.

Proteja seus dados, configure:

• Uma senha de bloqueio na tela inicial para que seja solicitado o código PIN;
• Faça backups periódicos para o Google Drive;
• Mantenha as informações sensíveis em formato criptografado;
• Desligue o WiFi e use os dados móveis do seu celular sempre que a comunicação envolver dados confidenciais.

Ao instalar aplicativos:

• Procure obter aplicativos de fontes confiáveis, como lojas oficiais ou o site do fabricante;
• Escolha aqueles que tenham sido bem avaliados e com grande quantidade de usuários;
• Verifique com seu programa antivírus antes de instalar um aplicativo;
• Observe se as permissões para a execução são coerentes com a finalidade do aplicativo (um aplicativo de jogos, por exemplo, não necessariamente precisa ter acesso a sua lista de chamadas.)

Ao acessar redes:

• Seja cuidadoso ao usar redes Wi-Fi públicas (desabilite a opção de conexão automática);
• Mantenha interfaces de comunicação, como bluetooth, infravermelho e Wi-Fi, desativadas (somente as habilite quando necessário);
• Configure a conexão bluetooth para que seu dispositivo não seja identificado (ou "descoberto") por outros aparelhos.

Em caso de perda ou furto, configure-o previamente, se possível para que:

• Seja localizado/rastreado e bloqueado remotamente, por meio de serviços de geolocalização;
• Uma mensagem seja mostrada na tela (para aumentar as chances dele ser devolvido);
• O volume seja aumentado ou que saia do modo silencioso (para facilitar a localização);
• Os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso;
• Informe sua operadora e solicite o bloqueio do seu número (chip);
• Informe a empresa onde você trabalha, caso haja dados e senhas profissionais nele armazenadas;
• Altere as senhas que possam estar nele armazenadas;
• Bloqueie cartões de crédito cujos números estejam nele armazenados;
• Ative a localização remota, caso você a tenha configurado se achar necessário, apague remotamente todos os dados nele armazenados.

Senhas

Por meio de contas e senhas os sistemas conseguem saber quem você é, confirmar sua identidade e definir as ações que você pode realizar.
A sua conta de usuário em um determinado sistema normalmente é de conhecimento público, já que é por meio dela que as pessoas e serviços conseguem identificar quem você é. Desta forma, proteger sua senha é essencial para se prevenir dos riscos envolvidos no uso da Internet, pois é o segredo dela que garante a sua identidade, ou seja, que você é o dono da sua conta de usuário.

Seja cuidadoso ao usar e ao elaborar as suas senhas:

• Use senhas longas, compostas de diferentes tipos de caracteres;
• Evite usar dados pessoais, como nome, sobrenome e datas;

Seja cuidadoso ao usar suas senhas:

• Certifique-se de não estar sendo observado ao digitá-las;
• Não as deixe anotadas em locais onde outras pessoas possam vê-las (por exemplo, em um papel colado no monitor do seu computador);
• Evite digitá-las em computadores e dispositivos móveis de terceiros;

Não forneça as suas senhas para outra pessoa, em hipótese alguma:

• Fique atento a ligações telefônicas e e-mails pelos quais solicitam informações pessoais sobre você, inclusive senhas;
• Certifique-se de usar conexões seguras sempre que o acesso envolver senhas;
• Evite salvar as suas senhas no navegador Web;
• Evite usar opções como "Lembre-se de mim" e "Continuar conectado";
• Evite usar a mesma senha para todos os serviços que você acessa.

Seja cuidadoso ao usar mecanismos de recuperação:

• Certifique-se de configurar opções de recuperação de senha, como um endereço de e-mail alternativo, uma pergunta de segurança e um número de telefone celular;
• Ao usar perguntas de segurança evite escolher questões cujas respostas possam ser facilmente adivinhadas;
• Ao usar dicas de segurança, escolha aquelas que sejam vagas o suficiente para que ninguém consiga descobri-las e claras o bastante para que você possa entendê-las;
• Ao solicitar o envio de suas senhas por e-mail altere-as o mais rápido possível e certifique-se de cadastrar um e-mail de recuperação que você acesse regularmente.

Proteja-se de phishing e códigos maliciosos:

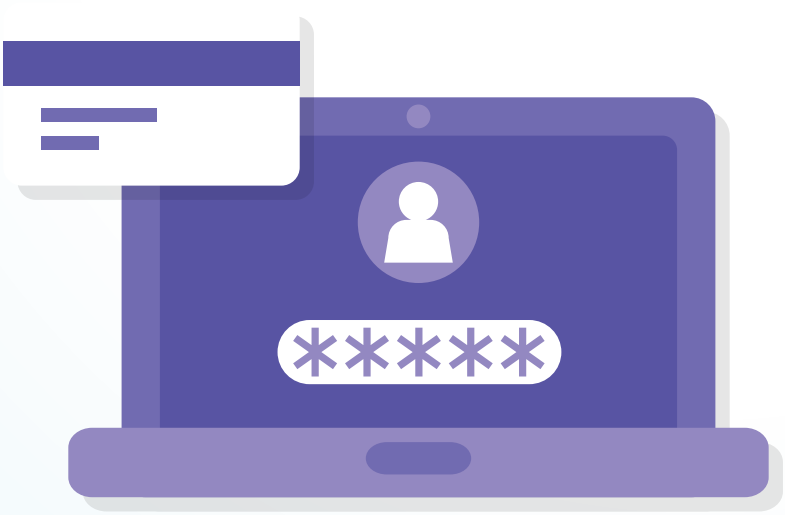
• Desconfie de mensagens recebidas, mesmo que enviadas por conhecidos;
• Evite seguir links recebidos em mensagens eletrônicas;
• Não utilize um site de busca para acessar serviços que requeiram senhas, como seu E-mail e suas redes sociais;
• Seja cuidadoso ao acessar links reduzidos.

Proteja seus dispositivos móveis:

• Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (composta de letras, números e caracteres);
• Em caso de perda ou furto altere as senhas que possam estar nele armazenadas.

Seja cuidadoso ao usar computadores de terceiros:

• Certifique-se de fechar a sua sessão (logout) ao acessar sites que usem senhas;
• Procure, sempre que possível, utilizar opções de navegação anônima;
• Evite efetuar transações bancárias e comerciais.



Redes Sociais

O acesso às redes sociais já está incorporado ao cotidiano de grande parte dos usuários da Internet e, muito provavelmente, do seu.

As redes sociais estão presentes nos mais diversos meios, como pessoal, profissional, econômico, político e jornalístico.

O sucesso das redes sociais, somadas a popularidade dos dispositivos móveis fizeram com que chamassem a atenção, também, de pessoas mal-intencionadas.

Por isso, para usar as redes sociais de forma segura, é muito importante que você esteja ciente dos riscos que elas podem representar e possa, assim, tomar medidas preventivas para evitá-los.

Proteja o seu perfil:

• Seja cuidadoso ao usar e ao elaborar as suas senhas;
• Habilite a notificação de login e a verificação em duas etapas, sempre que estes recursos estiverem disponíveis;
• Procure cadastrar um e-mail de recuperação que você acesse regularmente;
• Verifique o registro de atividades, caso desconfie que seu perfil tenha sido indevidamente usado;

Proteja a sua privacidade:

• Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa;
• Use as configurações de privacidade oferecidas pelos sites e seja o mais restritivo possível;
• Mantenha seu perfil e seus dados privados;
• Seja cuidadoso ao aceitar seus contatos e ao se associar a grupos;
• Não confie na promessa de anonimato oferecida por algumas redes sociais e aplicativos;
• Seja cuidadoso ao fornecer a sua localização, não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência;
• Ao usar redes sociais baseadas em geolocalização, procure fazer check-in apenas em locais movimentados e, de preferência, ao sair do local .

Proteja seus filhos:

• Informe seus filhos sobre os riscos de uso das redes sociais;
• Respeite os limites de idade estipulados pelos sites;
• Não exponha excessivamente seus filhos. O que para você pode ser algo inocente, para outras pessoas pode ter uma conotação diferente.

Proteja a sua vida profissional:

• Ao usar redes sociais profissionais (como o LinkedIn) procure ser formal e evite tratar de assuntos pessoais;
• Antes de postar algo avalie se, de alguma forma, aquilo pode atrapalhar a sua carreira;
• Verifique sempre a origem do conteúdo postado, levando sempre em consideração a veracidade;
• Verifique se sua empresa possui um código de conduta e evite divulgar detalhes sobre o seu trabalho.

Códigos Maliciosos

Códigos maliciosos também conhecidos como pragas e malware, são programas desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos, como computadores, modems, switches, roteadores e dispositivos móveis (tablets, celulares, smartphones, etc).

Após infectar o seu equipamento, o código malicioso pode executar ações como se fosse você, como acessar informações, apagar arquivos, criptografar dados, conectar-se à Internet, enviar mensagens e ainda instalar outros códigos maliciosos. A melhor prevenção contra os códigos maliciosos é impedir que a infecção ocorra pois nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente seus dados.

Cuidados a serem tomados, mantenha seus equipamentos atualizados:

• Use apenas programas originais;
• Tenha sempre as versões mais recentes dos programas instalados;
• Instale todas as atualizações disponíveis, principalmente as de segurança;
• Crie um disco de recuperação e tenha-o por perto no caso de emergências.

Instale um antivírus (antimalware):

• Mantenha o antivírus atualizado;
• Configure o antivírus para verificar automaticamente toda e qualquer extensão de arquivo, arquivos anexados aos e-mails, obtidos pela Internet, os discos rígidos e as unidades removíveis;
• Evite executar simultaneamente diferentes antivírus (eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro);
• Crie um ponto de restauração de seu sistema antes de começar a usar.
• Instale um antivírus mesmo que gratuito, os mais conhecidos são AVG, Avast e Avira.

Use um firewall pessoal:

• Assegure-se de ter um firewall pessoal instalado e ativo;
• Verifique periodicamente os logs do firewall à procura de acessos maliciosos.

Ao instalar aplicativos:

• Baixe aplicativos apenas de fontes confiáveis;
• Verifique se as permissões de instalação e execução são coerentes;
• Escolha aplicativos bem avaliados e com grande quantidade de usuários.

Faça backups:

• Proteja seus dados, fazendo backups regularmente;
• Mantenha os backups desconectados do sistema.

Seja cuidadoso ao clicar em links:

• Seja cuidadoso ao clicar em links, independente de como foram recebidos e de quem os enviou;
• Antes de clicar em um link curto procure usar complementos que possibilitem que o link de destino seja visualizado;
• Não considere que mensagens vindas de conhecidos são sempre confiáveis;
• O campo de remetente pode ter sido falsificado, ou elas podem ter sido enviadas de contas falsas ou invadidas.

Outros:

• Cuidado com extensões ocultas;
• Desabilite a auto-execução de mídias removíveis e de arquivos anexados.

Computadores

Muito provavelmente é em seu computador que a maioria dos seus dados está gravada e, por meio dele, que você acessa e-mails e redes sociais e realiza transações bancárias e comerciais, certo?
Manter seu computador seguro é essencial para se proteger dos riscos envolvidos no uso da Internet como ser invadido ou infectado.

Seja cuidadoso ao usar computadores de terceiros:

• Utilize opções de navegar anonimamente;
• Não efetue transações bancárias ou comerciais;
• Não utilize opções como "Lembre-se de mim" e "Continuar conectado";
• Não permita que suas senhas sejam memorizadas pelo navegador Web;
• Limpe os dados pessoais salvos pelo navegador;
• Assegure-se de sair (logout) de suas contas de usuário seja cuidadoso ao conectar mídias removíveis, como pen-drives.

Ao compartilhar recursos do seu computador, proteja suas contas de acesso e senhas:

• Crie uma conta padrão e use-a nas tarefas rotineiras;
• Use a conta de administrador somente quando necessário e pelo menor tempo possível;
• Use a opção de "executar como administrador" quando necessitar de privilégios administrativos;
• Assegure-se de que todas as contas de acesso existentes tenham senha não existam contas de uso compartilhado;
• Assegure-se de que a conta de acesso e a senha sejam solicitadas na tela inicial a opção de login automático esteja desabilitada.

SUPERINTENDÊNCIA DE
TECNOLOGIA DA INFORMAÇÃO

Universidade Federal Fluminense