Segurança da INFORMAÇÃO

saiba como proteger os seus dados

Guia prático de segurança de dados

INSTITUTO FEDERAL
Amapá

Guia prático de
segurança de dados

1 Spam

é o termo usado para se
referir aos e-mails não solicitados.

Identificação:

É importante identificar os spams para que se possa agir adequadamente. Geralmente possuem as seguintes características.

- Apresentam no campo “Assunto” (“Subject”) palavras com grafia errada ou suspeita: a maioria dos filtros antispam utilizam o conteúdo deste campo para barrar e-mails com assuntos considerados suspeitos.

- Apresentam no campo “Assunto” textos alarmantes ou vagos: na tentativa de confundir os filtros antispam e de atrair a atenção dos usuários, os spammers costumam colocar textos alarmantes, atraentes ou vagos demais, como “Sua senha está inválida”, “A informação que você pediu” e “Parabéns”.

Prevenção:

Não siga (clique) links recebidos em spams e não responda mensagens desse tipo (essas ações podem servir para confirmar que seu e-mail é válido).

- Desabilite a abertura de imagens em e-mails HTML (o fato de uma imagem ser acessada pode servir para confirmar que a mensagem foi lida).

- Crie contas de e-mail secundárias e forneça-as em locais onde as chances de receber spam são grandes, como ao preencher cadastros em lojas e em listas de discussão.

- Respeite o endereço de e-mail de outras pessoas. Use a opção de CCO (Cópia Oculta) ao enviar e-mail para grande quantidade de pessoas. Ao encaminhar mensagens, apague a lista de antigos destinatários, pois mensagens reencaminhadas podem servir como fonte de coleta para spammers.

Guia prático de segurança de dados

Senhas de segurança

***Senha ou password** serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão.*

Perigos

Se outra pessoa souber a sua conta de usuário e tiver acesso à sua senha, ela poderá usá-las para se passar por você na internet e realizar ações em seu nome, como:

- Acessar a sua conta de correio eletrônico e ler seus e-mails, enviar mensagens de spam e/ou contendo phishing e códigos maliciosos e furtar sua lista de contatos.

- Pedir o reenvio de senhas de outras contas para esse endereço de e-mail (e assim conseguir acesso a elas).

- Acessar o seu computador e obter informações sensíveis armazenadas nele, como senhas e números de cartões de crédito.

- Utilizar o seu computador para esconder a real identidade dessa pessoa (o invasor) e, então, desferir ataques contra computadores de terceiros.

Cuidados a serem tomados ao usar suas contas e senhas:

- Certifique-se de não estar sendo observado ao digitar as suas senhas.
- Não forneça as suas senhas para outra pessoa, em hipótese alguma.
- Certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senhas.

Use a opção de sair (logout), pois isso evita que suas informações sejam mantidas no navegador.

- Não use a mesma senha para todos os serviços que acessa.
- Elabore senhas fortes com no mínimo seis caracteres, alternando entre letras, números e caracteres especiais e :

1 - Não use qualquer tipo de dado pessoal.
2 - Não use sequências de teclado como:
- "1qaz2wsx" e "QwerTAsdfG".

Guia prático de
segurança de dados

Use apenas programas originais

A instalação de programas não originais, obtidos de mídias e sites não confiáveis ou via programas de compartilhamento de arquivos, pode incluir a instalação de códigos maliciosos, colocando em risco seu computador.

- Ao enviar seu computador para manutenção, não permita a instalação de programas que não sejam originais.

- Caso deseje usar um programa proprietário, mas não tenha recursos para adquirir a licença, procure por alternativas gratuitas ou mais baratas e que apresentem funcionalidades semelhantes às desejadas.

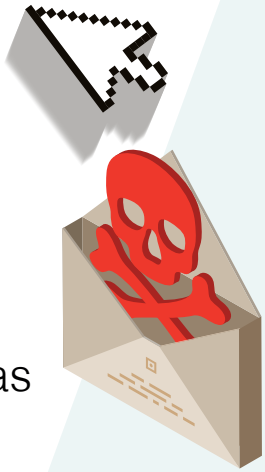
Diga não à **Pirataria,** é crime.

Diti Diretoria de Tecnologia da Informação
INSTITUTO FEDERAL
Amapá

Seja cuidadoso ao manipular arquivos

Alguns mecanismos, como os programas antimalware, são importantes para proteger seu computador contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas. Novos códigos maliciosos podem surgir a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança e, por isso, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas.

- Seja cuidadoso ao clicar em links, independentemente de como foram recebidos e de quem os enviou.



- Não considere que mensagens vindas de conhecidos são sempre confiáveis, pois o campo de remetente pode ter sido falsificado ou elas podem ter sido enviadas de contas falsas ou invadidas.

- Não abra ou execute arquivos sem antes verificá-los com seu antimalware.

Guia prático de segurança de dados

Bloquear a tela quando não estiver no mesmo ambiente do computador

Quando usar seu computador em locais públicos ou quando se ausentar do ambiente, é importante tomar cuidados para evitar que ele seja indevidamente utilizado por outras pessoas.

- Procure manter seu computador bloqueado, para evitar que seja usado quando você não estiver por perto (isso pode ser feito utilizando protetores de tela com senha; nos sistemas Windows a combinação WIN + L já é suficiente para habilitar essa proteção).

Guia prático de segurança de dados

Segurança em dispositivos móveis

Ao acessar redes:

- Seja cuidadoso ao usar redes wi-fi públicas.

- Mantenha interfaces de comunicação, como bluetooth, infravermelho e wi-fi, desabilitadas e somente as habilite quando for necessário.

- Configure a conexão bluetooth para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos essa opção aparece como "Oculto" ou "Invisível").

Guia prático de segurança de dados

Perda ou furto de celular, notebook ou desktop

O que fazer em caso de perda ou furto de celular, notebook ou desktop

- Informe a sua operadora e solicite o bloqueio do seu número (chip).

- Altere as senhas que possam estar armazenadas nele, como as de acesso ao e-mail, rede social e SUAP.

- Bloqueie cartão de crédito cujo número esteja armazenado em seu dispositivo móvel.

- Se estiver configurada a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados nele armazenados com auxílio de softwares especializados previamente instalados.

Diti Diretoria de Tecnologia da Informação
INSTITUTO FEDERAL Amapá

Guia prático de segurança de dados

Pishing

Phishing, phishing-scam ou phishing/scam *é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social.*

Atenção

Para atrair a atenção do usuário, as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento. Exemplos de situações envolvendo phishing são:

- Páginas falsas de comércio eletrônico ou internet banking;
- Páginas falsas de redes sociais ou de companhias aéreas;
- Mensagens contendo formulários;
- Solicitação de recadastramento.

Prevenção:

- Fique atento a mensagens recebidas em nome de alguma instituição que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links.

- Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança).

- Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos.

- Seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador web.

- Verifique se a página utiliza conexão segura. Sites de comércio eletrônico ou internet banking confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados.

Diti Diretoria de Tecnologia da Informação
INSTITUTO FEDERAL Amapá

Guia prático de segurança de dados

Sinais de comprometimento com a senha ou equipamento do instituto

A qualquer sinal de comprometimento de segurança de credenciais ou de equipamento do Instituto, entrar em contato com a TI de sua unidade.

Mantenha seus sistemas atualizados

Novas ameaças e vulnerabilidades são descobertas todos os dias. Logo, para proteger-se dessas, você deve manter seu sistema operacional e seus aplicativos sempre atualizados.

Procure por atualizações automáticas diretamente nas opções do software ou sistema operacional, ou baixe as atualizações regularmente a partir do fornecedor oficial. Sempre dê preferência para o site oficial do fornecedor.

Guia prático de segurança de dados

Uso adequado do e-mail institucional

O sigilo da sua senha é responsabilidade do servidor.

- Não use o e-mail institucional para tarefas não profissionais, como campanhas, promoções e redes sociais.

- A qualquer indício de anormalidade, redefina sua senha. (Fundamento: IN nº 1 DITI/2016, 5.8 e 5.9)

Obs.: A fundamentação mencionada está no portal do Ifap e pode ser obtida no link abaixo. https://portal.ifap.edu.br/

Seguindo estas dicas seus dados sempre estarão seguros.

O Ifap possui todos os procedimentos que envolvem a TI normatizados e publicados no endereço:
https://portal.ifap.edu.br/index.php/publicacoes/itemlist/category/45-documentos-diti

Guia prático de segurança de dados

Diti

Diretoria de Tecnologia da Informação

INSTITUTO FEDERAL
Amapá

10 ANOS