

CeTI-RP / STI

USP

Cartilha de boas
práticas para o
uso de emails e
segurança da
informação



Universidade de São Paulo
Reitor
Prof. Dr. Marco Antonio Zago

Vice-Reitor
Prof. Dr. Vahan Agopyan

Campus de Ribeirão Preto
Prefeito do Campus
Prof. Dr. Osvaldo Luiz Bezzon

Superintendência de Tecnologia da Informação
Superintendente
Prof. Dr. João Eduardo Ferreira

Centro de Tecnologia da Informação de Ribeirão Preto
Diretor
Prof. Dr. Alexandre Souto Martinez

Colaboradores Técnicos:
Ali Faiez Taha
Claudia Helena Bianchi Lencioni
Juliano alves Guidini
Robson Eisinger

Revisora
Clélia Camargo Cardoso

Apoio
IEA-RP

Diagramação
João Henrique Rafael

Introdução

O correio eletrônico é o serviço mais utilizado na Internet atualmente. Estima-se que 500 bilhões de e-mails circulem diariamente. Deste volume todo 86% é considerado spam e o restante, apenas 14%, são e-mails legítimos.

Definições:

Malwares

Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. O e-mail pode ser um veículo para um malware disfarçado de arquivo anexo ou conter um link que ao ser aberto, remete ao software mal intencionado;

Spam

São e-mails não solicitados, enviados para um grande número de pessoas. Fazendo uma analogia, quando um morador abre a caixa de correio de sua casa e encontra 20 panfletos de pizzeria, 11 de entrega de gás, 5 de imobiliária, etc. Ele separa as correspondências e permanece apenas com aquilo que é necessário. No caso do e-mail o usuário precisa selecionar o que não for necessário e mover para a pasta spam, com isso ele vai definindo o sistema de filtros antispam;

E-mail Spoofing

Técnica que consiste em alterar

campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra;

E-mail marketing

Utilizado para fazer marketing (propaganda) de produtos comerciais;

Phishing

É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário. Geralmente um link no corpo do texto que remete a um formulário (que captará informações pessoais) ou à instalação de um malware;

Newsletter

Lista de e-mails onde diversos participantes inscritos discutem determinado assunto;

Hoax

E-mails relacionados a boatos, fofocas e lendas urbanas;

STARTTLS

É uma forma de estabelecer uma conexão segura usando TLS ou SSL. Ambos fornecem uma maneira de criptografar um canal de comunicação entre dois computadores. TLS é um protocolo que assegura a privacidade na comunicação do usuário. Ele garante que nenhum terceiro possa interceptar, adulterar ou espionar um e-mail.

Recomendações básicas ao receber um e-mail

- Não responda a e-mails que solicitam recadastramento de senhas, dados de conta bancária, de cartão de crédito, prêmios, promoções, sorteios, brindes, informações pessoais, informações confidenciais, documentos de identidade, CPF e outros que pareçam suspeitos;
- Não abra e-mails de procedência desconhecida;
- Não abra ou responda mensagens consideradas spam; se a mensagem for spam, marque-a;
- Cuidado com arquivos anexados ao e-mail (principalmente com extensão .exe, .scr, .com, .bat, .doc, .dot, .xls, .mdb entre outras) que podem ser malwares (programas mal intencionados). A mensagem também pode conter redirecionamento para sites não confiáveis;
- Faça uma verificação criteriosa sobre a empresa ou pessoa que esteja solicitando informações e, na dúvida, não responda ao solicitado. Em caso de suspeita, delete imediatamente a mensagem do seu computador;
- Antes de abrir qualquer arquivo anexo, mesmo que de origem conhecida, verifique-o com um software antivírus, que deve estar sempre ativo e atualizado;
- Não abra arquivos anexos ao e-mail cujo título informe sobre fotos de uma celebridade, morte ou acidente de um artista, calamidades, etc. Estes assuntos bombásticos são alvos de golpistas e fraudadores;
- Não responda e-mails de bancos ou instituições financeiras. Essas empresas não se comunicam através de e-mails, pois possuem canais de relacionamentos que são divulgados aos clientes. Se tiver dúvidas sobre a legitimidade de uma mensagem, entre em contato com a pessoa ou instituição para ter certeza de que não se trata de uma fraude;
- Se não quiser receber propagandas não divulgue seu e-mail institucional em lojas ou qualquer estabelecimento comercial físico ou virtual;
- Em sites institucionais, evite expor diretamente os emails, existem robôs especializados na extração de e-mails. Utilize formulários de contato ou então imagens, para dificultar a ação desses robôs;
- Evite expor o email em redes sociais;



♦ Características que tornam um e-mail suspeito:

- **Campos “De: e Para:”**

- Os campos de remetente e/ou destinatário aparecem vazios ou com apelidos/nomes genéricos como "amigo@" e "suporte@";

- **Campo “CC, CCO, BCC:”**

- Segue a mesma regra acima;

- **Campo “Título, Assunto:”**

- A maioria dos filtros antispam utiliza o conteúdo deste campo para barrar e-mails com assuntos considerados suspeitos. No entanto, os spammers adaptam-se e tentam enganar os filtros colocando neste campo conteúdos enganosos, como “vi@gra” (em vez de “viagra”). Desconfie de textos com grafias erradas;

- Desconfie de e-mails cujo título/assunto contenha as palavras Sir, Madam, Sexo, Viagra, Milion Dolars, Nota Fiscal, Cobrança, Boleto, Serasa, entre outras;

- **Campo “Texto:”**

- 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", "Parabéns", entre tantos outros;

- Alguns spams tentam justificar o abuso, alegando que é possível sair da lista de divulgação, clicando no endereço anexo ao e-mail. Este artifício, porém, além de não retirar o seu endereço de e-mail da lista, também serve para validar que ele realmente existe e que é lido por alguém;

- Alguns spams prometem que serão enviados "uma única vez", ao alegarem isto, sugerem que não é necessário que você tome alguma ação para impedir que a mensagem seja novamente enviada;

- **Anexo**

- Procure salvar o arquivo recebido no seu computador e verifica-lo com o antivírus antes de abri-lo, até mesmo de origem conhecida.

Recomendações básicas ao enviar um e-mail

- As chaves para um bom e-mail são clareza, concisão e precisão;

- Recomendações para o preenchimento dos campos:

- **Campo “Para:”**

- Não é recomendável enviar e-mails para muitos usuários. Quando existe um número alto de e-mails nesse campo, é colocada uma pontuação que associada com a pontuação de outros campos pode considerar esse e-mail um spam;

- Utilize o menor número de destinatários possível, geralmente número máximo de 25 destinatários;

- Sempre que precisar enviar para vários destinatários faça uso de listas de distribuição;

- Faça uso do compartilhamento de arquivos, portanto evite encaminhar anexos de grande tamanho;

- **Campo “CC, CCO, BCC:”**

- Segue a mesma regra acima;

- **Campo “Título, Assunto:”**

- Escreva um título curto e preciso para o assunto de seu e-mail, construa o título com letras maiúsculas e minúsculas;

- Certifique-se de que o título esteja claro mesmo para alguém que desconhece você completamente. Se possível, inclua a palavra-chave que fará com que o conteúdo do e-

mail seja mais fácil de lembrar e procurar caso a caixa postal do destinatário esteja lotada;

- Não crie um título com apenas letras maiúsculas, existe uma pontuação para cada campo, que associada com outros campos pode considerar esse e-mail um spam;

- Evite enviar e-mail com o campo "assunto" vazio;

- Essas recomendações, com mais detalhes, podem ser vistas no site: <http://pt.wikihow.com/Escrever-um-E%E2%80%90mail-Formal>

- **Campo “Texto:”**

- Escreva a mensagem de modo que os destinatários possam entender o que você realmente quer dizer, entender o conteúdo da mensagem e o que anexou. O e-mail deve ser simples e curto, com poucos parágrafos;

- Evite usar o recurso de cópia de textos, o CONTROL-C e CONTROL-V. Isso pode trazer caracteres estranhos e símbolos indecifráveis na mensagem. É melhor anexar o texto que pretende enviar na mensagem como arquivo, pois mantém o conteúdo e formato sem modificações;

- Evite o clique compulsivo, isto é, clicar em mensagens recebidas e repassá-las instantaneamente, sem ler previamente e não saber a origem, se tem vírus ou não, se é



spam ou hoax, propagandas ou outros tipos de e-mails citados anteriormente;

Veja mais informações em:
www.facebook.com/truzziadvogados/posts/737993649560096

- Lembre-se de que e-mail é uma mensagem. Para escrever mensagens longas prepare um texto que o destinatário possa ler e entender, e envie-o como anexo;
- Use o editor padrão, não use HTML, para evitar caracteres estranhos na mensagem que podem comprometer a avaliação pelos filtros antispam;
- Evite colocar palavras já manjadas utilizadas pelos e-mails tipo spam (Viagra, Sexo, Nota Fiscal, Cobrança, Boleto, Serasa, etc.) pois existe uma pontuação para cada campo que associada com outros campos pode considerar esse e-mail um spam;
- Evite colocar fotos e imagens. Envie esses arquivos sempre em anexo e devidamente verificados pelo antivírus;

• **Anexo**

- Faça uso, preferencialmente, do compartilhamento de arquivos, portanto evite encaminhar anexos de grande tamanho;

• **Rodapé**

- Evite uso de figuras, GIFs animadas, textos formatados, cores diferentes;
- No rodapé utilize apenas seu nome e dados para que a pessoa possa se comunicar com você, como os telefones, cargo e local onde trabalha.

ATENÇÃO: Um e-mail é considerado spam através do somatório de pontos relacionados a cada campo, e se seu e-mail for considerado spam a instituição entra em uma ou mais black lists. Quando a instituição entra para uma black list, os e-mails enviados por você não serão recebidos nas contas dos destinatários. Isso causa um transtorno para você, para o departamento, para a Unidade e para Universidade. Geralmente para uma instituição sair de uma black list leva em torno de 12-24 horas.

Recomendações básicas na utilização do webmail

Webmail é a forma mais segura de enviar e receber e-mails;

- Utilize o menor número de destinatários possível, geralmente número máximo de 25 destinatários;
- Sempre que precisar enviar para vários destinatários faça uso de listas de distribuição;
- Faça uso do compartilhamento de arquivos, portanto evite encaminhar anexos de grande tamanho;
- Seja cuidadoso ao acessar a página de seu webmail para não ser vítima de phishing. Digite a URL (endereço do site) diretamente no navegador e tenha cuidado ao clicar em links recebidos por meio de mensagens eletrônicas;



- Não utilize um site de busca para acessar seu webmail;
- Seja cuidadoso ao elaborar sua senha de acesso ao webmail para evitar que ela seja descoberta por meio de ataques de força bruta (algoritmos que testam senhas curtas);
- Configure as opções de recuperação de senha: endereço de e-mail alternativo, uma questão de segurança e um número de telefone celular;
- Evite acessar seu webmail em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anônima (recurso usado para quem quer usar a Internet sem que seus dados e cookies sejam salvos no histórico);
- Certifique-se de utilizar conexões seguras, ou seja que requeiram autenticação, sempre que acessar seu webmail, especialmente ao usar redes wi-fi públicas;
- Instalar componentes do navegador apenas de sites confiáveis, pois podem conter códigos maliciosos;
- Desabilite em “Preferências” a exibição de imagens automaticamente porque o código HTML que contém a imagem pode conter malwares que são executados sem o clique do usuário.

Recomendações básicas na utilização de programas leitores de e-mail: (Outlook, Thunderbird, Opera Mail, etc.)



- Mantenha o programa leitor de email atualizado com a versão mais recente e com as todas atualizações aplicadas;
- Configure-o para verificar automaticamente atualizações, tanto dele próprio como de complementos que estejam instalados;
- Não o utilize como navegador Web (desligue o modo de visualização no formato HTML, pois pode executar códigos automaticamente);
- Seja cuidadoso ao usar cookies caso deseje ter mais privacidade;
- Seja cuidadoso ao clicar em links presentes em e-mails (se você realmente quiser acessar a página do link, digite o endereço diretamente no seu navegador Web);
- Desconfie de arquivos anexados à mensagem mesmo que tenham sido enviados por pessoas ou instituições conhecidas (o endereço do remetente pode ter sido falsificado e o arquivo anexo pode estar infectado);
- Antes de abrir um arquivo anexado à mensagem tenha certeza de que ele não apresenta riscos, verificando-o com ferramentas antivírus;
- Desligue as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens como, por exemplo, execução de Java Script e de programas Java;
- Habilite, se possível, opções para marcar mensagens suspeitas de serem fraude;
- Use sempre criptografia para conexão entre seu leitor de e-mails e os servidores de e-mail do seu provedor. É necessário configurar o tipo de conexão criptografada no programa leitor de e-mail, no momento a mais utilizada é STARTTLS. Para configurar é necessário acessar “Propriedades” na conta de e-mail.

Cuidado com as senhas



- Nunca divulgue sua senha e evite anotá-la em pedaços de papel e deixa-la em local onde todos possam vê-la. **Senha sempre foi e sempre deve ser secreta;**

- Escolha uma senha que não seja sequência de números, palavras óbvias, nomes, placa de carro, número de telefone, etc. Uma senha não pode ser de fácil adivinhação ou muito óbvia. Adote senhas com pelo menos oito caracteres, misturando sempre caracteres alfanuméricos e símbolos presentes no teclado;

- Na composição de uma senha não é recomendável usar tecla de espaço e os símbolos ° e ^ e caracteres que exigem duas teclas para aparecer quando se digita, por exemplo:

^ ~ ' ` ¢ , ou seja, acentuação;

- Não utilize palavras que constam em dicionários, de qualquer língua, pois existem programas de quebra de senhas que utilizam dicionários;

- Troque suas senhas constantemente; no mínimo a cada três meses;

- Não deixe suas senhas armazenadas nos aplicativos para trabalhar com e-mails, em dispositivos móveis, telefone celular, tabletes, etc.;

- No leitor de e-mails (Thunderbird, Outlook, etc.) **opte por não armazenar a senha**, pois se outra pessoa utilizar seu computador terá acesso a seus e-mails.

- **Número aproximado de contas de e-mail: 220.000**

- **Cotas padrões para usuários:**

Alunos de Graduação: 300 MB

Alunos de Pós-Graduação: 1 GB

Funcionários: 1 GB

Docentes: 10 GB

- Tamanho máximo do anexo: não encaminhar anexos acima de 25 MB. Faça uso do serviço de compartilhamento de arquivos do Zimbra USP.

Caso tenha dúvidas técnicas, abaixo links com informações sobre os recursos de porta-arquivose compartilhamentos do Zimbra:

<http://www.dti.usp.br/atendimento/faq/uspmail/porta.html>

<http://www.dti.usp.br/atendimento/faq/uspmail/compartilhamento.html>

- **Contas Inativas:**

Para desativar uma conta de e-mail, a Unidade deve encaminhar e-mail ou ofício informando o desligamento e

solicitando o bloqueio do docente ou funcionário, e a conta será bloqueada. Do contrário a conta de e-mail continua ativa.

Se o usuário (docente, funcionário ou aluno) não acessa a conta há 6 meses, a conta é bloqueada. Se ele utiliza forward, a conta não é bloqueada e continua ativa.

Contas de comissões, órgãos e aposentados não são bloqueadas, a não ser que fiquem 6 meses inativas;

- Se esquecer a senha do e-mail @unidade.usp.br ou @usp.br, e não estiver em webmail.usp.br, acesse <https://webmail.usp.br>, a seguir clique em [esqueci a senha], digite o número USP e a senha única, então aparecerá uma tela solicitando que você digite uma nova senha de e-mail, ou entre em <http://pedidoemail.usp.br>, e haverá uma tela para você digitar uma nova senha de e-mail.

- Dúvidas quanto ao e-mail @usp.br ou @unidade.usp.br

<http://www.dti.usp.br/atendimento/faq/uspmail/index.html>

Como você pode ser afetado pelos problemas causados pelos spams:

- **Perda de mensagens importantes:** devido ao grande volume de spam recebido, você corre o risco de não ler mensagens importantes, lê-las com atraso ou apagá-las por engano;
- **Conteúdo impróprio ou ofensivo:** como grande parte dos spams são enviados para conjuntos aleatórios de endereços de e-mail, é bastante provável que você receba mensagens cujo conteúdo considere impróprio ou ofensivo;
- **Gasto desnecessário de tempo:** para cada spam recebido, é necessário que você gaste um tempo para lê-lo, identificá-lo e removê-lo da sua caixa postal, o que pode resultar em gasto desnecessário de tempo e em perda de produtividade;
- **Não recebimento de e-mails:** caso o número de spams recebidos seja grande e você utilize um serviço de e-mail que limite o tamanho de caixa postal, você corre o risco de lotar a sua área de e-mail e, até que consiga liberar espaço, ficará impedido de receber novas mensagens;
- **Classificação errada de mensagens:** Algumas mensagens

legítimas podem ser classificadas como spam, por isto o usuário deve examinar o conteúdo da pasta spam antes de esvaziá-la

Cuidados para reduzir o spam

- Procure filtrar as mensagens indesejadas, por meio de programas instalados em servidores ou em seu computador e de sistemas integrados a webmails e leitores de e-mails;
- Seja criterioso ao classificar uma mensagem como spam;
- Selecionar o e-mail que é necessário, o que não for necessário (propagandas, convites, sorteios, etc.), encaminhar para a pasta spam, com isso o usuário vai definindo o sistema de filtro antispam, que atua baseado em estatísticas;
- É importante que você, de tempos em tempos, verifique a pasta spam, pois podem acontecer casos de falsos positivos e mensagens legítimas virem a ser classificadas como spam. Caso você, mesmo usando filtros, receba um spam, deve classificá-lo como tal, pois estará ajudando a treinar o filtro;
- Seja cuidadoso ao fornecer seu endereço de e-mail. Existem situações onde não há motivo para que o seu e-mail seja fornecido. Ao preencher um cadastro, por

exemplo, pense se é realmente necessário fornecer o seu e-mail e se você deseja receber mensagens deste local;

- Fique atento a opções pré-selecionadas. Em alguns formulários ou cadastros preenchidos pela Internet, existe a pergunta se você quer receber e-mails, por exemplo, sobre promoções e lançamentos de produtos, cuja resposta já vem marcada como afirmativa. Fique atento a esta questão e desmarque-a, caso não deseje receber este tipo de mensagem;
- Não siga links recebidos em spams e não responda mensagens deste tipo (estas 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;
- Utilize as opções de privacidade das redes sociais (algumas redes permitem esconder o seu endereço de e-mail ou restringir as pessoas que terão acesso a ele);
- Respeite o endereço de e-mail de outras pessoas. Use a opção de "Bcc:" ao enviar e-mail para grandes quantidades de pessoas. Ao encaminhar mensagens, apague a lista de antigos destinatários, pois mensagens reencaminhadas podem servir como fonte de coleta para spammers.



Recomendações CeTI-SP 'SPAM'

De acordo com informação do CeTI-SP, reduzir a quantidade de SPAM recebida, é um trabalho que envolve a colaboração de todos os usuários.

As solicitações para análise de e-mails suspeitos são recebidas, dando prioridade às mensagens de scam/phishing, por envolver risco de comprometimento de contas no sistema.

Para facilitar o encaminhamento desse tipo de mensagem para análise, foi criado o seguinte e-mail de contato:

notifica.spam@usp.br

No webmail USP, existem duas formas de encaminhar a mensagem original para análise:

1) Na lista de mensagens, selecione a mensagem suspeita, clique com o botão direito sobre ela e escolha a opção "Exibir Original" (ou o equivalente no idioma usado no webmail).

Uma janela deve abrir com a mensagem original (contendo os cabeçalhos), caso a janela não

abra verifique se existe algum bloqueio de pop-up. Basta copiar o texto dessa mensagem e encaminhar para a conta de notificação de spam.

2) Caso sejam várias mensagens, selecione cada uma delas e clique na opção Encaminhar. Envie a mensagem para a conta de notificação de SPAM, as mensagens suspeitas serão encaminhadas como anexo.

ATENÇÃO:

Para facilitar o trabalho de análise, no campo Assunto/Subject, informe se é uma mensagem de SPAM (mail marketing) ou SCAM/PHISHING (mensagem pedindo usuário e senha ou informações pessoais do usuário), é recomendado enviar para o **security@usp.br** mensagens de SCAM/PHISHING, isto é, mensagens que solicitam dados pessoais como usuário e senha, seja diretamente na mensagem ou por meio de formulários, para que se possa registrar e dar prioridade ao atendimento.

Norma para uso das contas de correio eletrônico na USP

security.usp.br/normas_pseg03.html

Cartilhas sobre segurança na Internet e spam

www.cartilha.cert.br

www.antispam.br

Normas, recomendações e procedimentos de segurança

www.security.usp.br

Escrever um e-mail formal:

pt.wikihow.com/Escrever-um-E%E2%80%90mail-Formal

Vídeos

Zimbra webmail

https://www.youtube.com/results?search_query=Zimbra+webmail

Como configurar filtro de e-mails Zimbra webmail

<https://www.youtube.com/watch?v=ISz-ZdbaCrA>

Tutorial webmail Zimbra - Como bloquear spam.

<https://www.youtube.com/watch?v=qUxLNWWFiC4>

Como enviar e-mail

https://www.youtube.com/watch?v=_LPqZoLleLw#t=68

Como mandar um email - para iniciantes

<https://www.youtube.com/watch?v=tbXSksSX26k>

C o m o e n v i a r e - m a i l corretamente

<https://www.youtube.com/watch?v=fB2iOaikTPQ>

Como enviar arquivos por e-mail (anexo)

<https://www.youtube.com/watch?v=tsJpWZUL56U>

Como escanear e enviar um documento por e-mail

https://www.youtube.com/watch?v=_wHLHavNTno

Aprenda E Dicas: Uso profissional do e-mail

<https://www.youtube.com/watch?v=ztW7HyCtJNc>

Comunicação em Cena - Ep. 04: e-mail também é documento

<https://www.youtube.com/watch?v=1UWICo7PDXU>

