2019

Marcelo Garcia

NTI FURG

Sumário

1 Boas práticas na utilização do FURGMail

2 Escrita do e-mail

O e-mail hoje enquanto ferramenta de trabalho manifesta muitas vezes instruções e informações diretas, portanto temos que ter algum cuidado tanto no conteúdo, quanto em sua escrita.

- ➔ Evite uso de gírias, abreviações e linguagem coloquial.
- ➔ Seja objetivo.
- ➔ Revise o e-mail antes de enviar. É muito comum por exemplo o envio de mensagens que deveriam ter algum anexo, sem a sua efetiva incorporação no e-mail.
- ➔ Outra boa prática é enviar anexos legíveis com menor tamanho possível.
- ➔ Evite o uso do e-mail corporativo para assuntos pessoais.
- ➔ Releia a mensagem antes de enviá-la.

Preserve sempre a privacidade. Não revele dados pessoais e privados (siape, matricula, senhas, número de telefone,…) principalmente por e-mail.

É necessário atenção no envio de mensagens para um grande número de e-mails. A politica do FURGMail é classificar como SPAM o envio de 400 e-mails em um intervalo de tempo inferior a 2 horas, será classificado como *SPAMMER.*

Outra dica importante é não utilizar a conta de e-mail institucional para cadastros em redes sociais.

3 Netiqueta[1]

A netiqueta – a “etiqueta digital” ou “etiqueta da internet” – é um conjunto de regras sociais – formais ou informais; convencionadas ou naturais - que regulam o comportamento e a comunicação dos utilizadores da internet, promovendo a qualidade da socialização e a eficácia comunicativa, com origem em uma dissertação de mestrado da universidade do Porto em 2013.

Seu objetivo foi de apresentar uma classificação exaustiva das regras da netiqueta. Estruturada em regras básicas e as regras gerais da netiqueta discute a vida em sociedade no ciberespaço abordando questões relacionadas diretamente com a netiqueta, a privacidade, a incivilidade e o ciberbullying.

Do conjunto de pouco mais de 150 regras da Netiqueta disponivel no anexo 1, selecionamos o 15 relativos ao serviço de e-mail.

1 https://sigarra.up.pt/flup/pt/pub_geral.show_file?pi_doc_id=15174

44 - Não usar o email para comunicar más notícias.

45 - Não enviar emails possivelmente embaraçosos.

46 - Rever sempre o conteúdo do email antes do envio.

47 - Dizer no “assunto” o suficiente para que o destinatário fique com uma ideia precisa do conteúdo do email.

48 - Utilizar a função BCC em envios para um grande número de destinatários.

49 - Diferenciar os destinatários entre “Para” e “CC”.

50 - Usar os nomes completos juntamente com os endereços de email.

51 - Responder prontamente aos emails.

52 - Não começar uma nova mensagem para responder a um email.

53 - Não reencaminhar emails privados.

54 - Não alterar o texto de emails a reencaminhar.

55 -Utilizar, ou manter, as designações “RE” ou “FW” para as respostas ou reencaminhamentos, respetivamente.

56 - Não reencaminhar emails indiscriminadamente.

57 - Não ler os emails privados dos outros.

58 - Não usar métodos para obter notificações de quando os destinatários abrem o email enviado

4 E-mails maliciosos

Fazer ataques a servidores de instituições tende a ser um processo que demande tempo e estudo, o que leva os golpistas a explorarem as fragilidades dos usuários.

É importante frisar que o NTI FURG **jamais** enviará e-mails solicitando a sua senha, recadastramento de conta, contas, ou similares. Caso seja necessário usaremos canais formais da instituição, como vincular noticia via SECOM. E-mails com estas solicitações têm a intenção de explorar a engenharia social, portanto sempre desconfie de mensagens (e-mails) que contêm anexos ou links, principalmente se:

- Oferecem vantagens ou dinheiro rápido promoções;
- Alterações de senhas de banco;
- Fotos;
- Cobranças, boletos bancários..etc..

- Não clique em links que apareçam no conteúdo da mensagem de correio eletrônico. Esse procedimento é especialmente importante em mensagens cuja origem não seja absolutamente fidedigna. O endereço que aparece no texto pode ser facilmente reencaminhado para seus contatos, pode conter vírus ou outras “pragas virtuais”.

Apague-as e, principalmente, não caia na tentação de responder ou fazer download de anexos, isso confirmará a existência da sua conta.

A exemplo, citamos a técnica de *phishing* que utiliza cartas falsas de entidades bancárias ou instituições financeiras com links redirecionados e que levam os usuários a divulgar dados sensíveis.

Não se transforme em um *spammer*, reenviando correntes da sorte, distribuindo boatos (hoaxes), divulgando informações que podem NÃO ser do interesse dos seus contatos. Grande parte dessas mensagens também possuem vírus ou “pragas digitais”, não dissemine-as.

Desconfie sempre dos arquivos enviados em anexo, mesmo que a origem seja conhecida, pelo fato de o endereço do remetente poder ter sido forjado; trata-se de um esquema utilizado por intrusos, chamado *spoofing*. A seguir vemos exemplos reais de *spoofing* e *phishing*.

From: FURG <abido@matrix.com.br>
Date: qui, 21 de mar de 2019 às 10:31
Subject: Aviso de atualização de e-mail
To:

Prezado usuário da FURG,

Sua caixa de correio excedeu o limite de armazenamento normal de 100 MB, você não poderá receber nem enviar emails até aumentar sua cota de caixa de correio. Para aumentar sua cota de e-mail, CLIQUE AQUI e preencha os detalhes necessários para aumentar sua cota de caixa de correio.

Após 48 horas sem receber qualquer resposta sua, sua caixa de correio será desativada temporariamente.

Obrigado por usar nosso webmail

Copyright © 2019 O Serviço de Admin,

De: "FURG ADMIN" <rzn.zarpelao@unifesp.br>
Data: 9 de jan de 2017 2:45 PM
Assunto: FURG Universidade.
Para:
Cc:

Caro usuário de e-mail,

Esta mensagem é para informar todos os nossos funcionários e alunos da FURG
Titulares de contas de e-mail da Universidade. Começamos a atualizar nossos
Banco de dados do servidor e centro do servidor de contas de e-mail. Estamos cancelando
Conta de e-mail webmail não utilizada imediatamente para criar mais
Novas contas de funcionários e alunos. Para evitar que sua conta
Fechamento você terá que atualizá-lo abaixo para que nós saibamos que é
Status como uma account.please atualmente usado atualizar sua conta em 48 horas com o link abaixo para evitar o encerramento permanetly.

Clique aqui para confirmar as suas contas.

Https://activemailuser.000webhostapp.com

**** A ligação Acima não funciona? ****

Se o link acima não funcionar, copie e cole o URL seguinte em

Seu navegador. Https://activemailuser.000webhostapp.com

Obrigado pela sua compreensão enquanto trabalhamos juntos para proteger

sua conta.

Feliz ano novo para você e sua família.
© Universidade Federal do Rio Grande - FURG

De: amministratore di sistema <ciatox@msp.gob.ec>
Date: ter, 31 de jan de 2017 às 13:19
Subject: Atualize seu e-mail
To:

Sua caixa de correio excedeu o limite de armazenamento é de 1 GB, que é definido
pelo administrador, estão sendo executados em 99,8 gigabytes,
você não pode enviar ou receber novas mensagens até
que você re-validar sua caixa de correio. Para renovar a
caixa de correio, clique no link abaixo e preencha as informações para confirmar sua conta.

http://gracia-listello.co.id/br/public_html/webmail/webmail/index.php

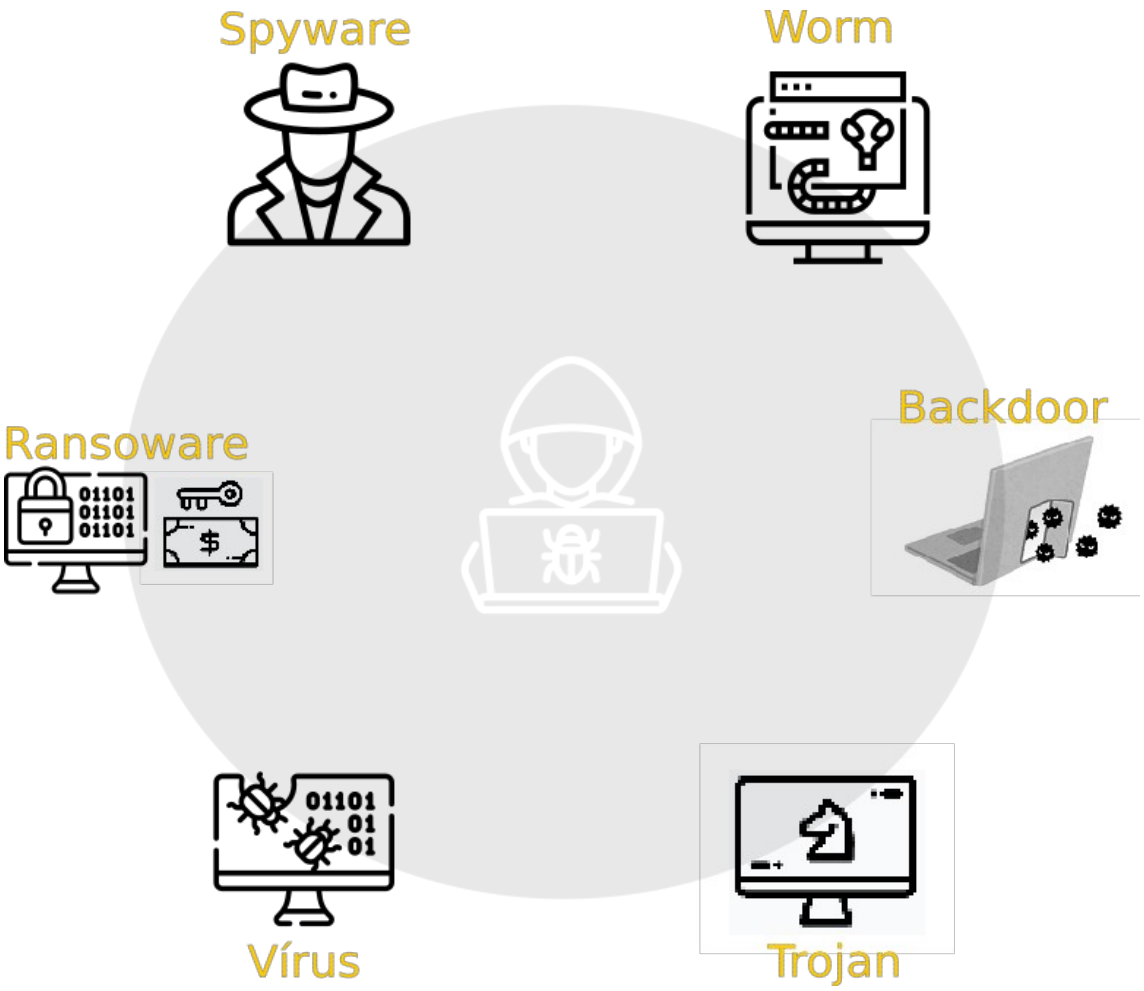
Obrigado!
Web mail administrador de sistema!
ATENÇÃO! Proteja sua privacidade.
Sair quando terminar e completamente

Nota de Descargo: La informacion contenida en este mensaje y sus anexos tiene caracter confidencial, y esta dirigida unicamente al destinatario de la misma y solo podra ser usada por este. Si el lector de este mensaje no es el destinatario del mismo, se le notifica que cualquier copia o distribucion de este se encuentra totalmente prohibida. Si usted ha recibido este mensaje por error, por favor notifique inmediatamente al remitente por este mismo medio y borre el mensaje de su sistema. Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinion oficial del MINISTERIO DE SALUD del Ecuador.

2 Segurança da informação

2.1 Malwares

Existe uma diversidade de pragas virtuais, compiladas de forma sucinta na figura 1, e são chamados de Malware (abreviatura para “software malicioso”).



Segundo a AVAST, Os tipos de malware incluem spyware, adware, phishing, vírus, Cavalos de Tróia, worms,ramsoware e sequestradores de navegador. Os conceitos a seguir são baseados no site da AVAST[2], PANDA[3] e Kaspersky[4]

2 https://www.avast.com/pt-br/c-online-threats

3 https://www.pandasecurity.com/en/security-info/

4 https://www.kaspersky.com.br/resource-center

- Vírus é programa ou pedaço de código que é carregado ao seu computador sem seu conhecimento ou permissão. Alguns vírus são meramente irritantes, mas a maioria dos vírus são destrutivos e designados a infectar e controlar sistemas vulneráveis. Um vírus pode se alastrar a vários computadores e redes ao criar cópias dele mesmo, assim como um vírus biológico passa de uma pessoa para a outra.

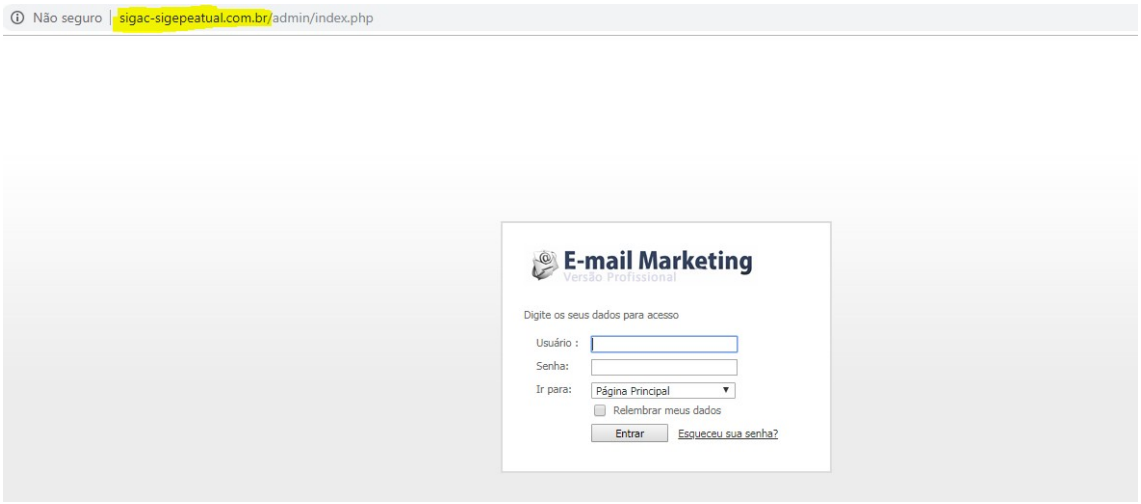
- Um Trojan Horse (Cavalo de Tróia) é um tipo de vírus que pretende ser útil ou divertido enquanto na verdade causa problemas e rouba dados.

- O backdoor é um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada. Para esse fim, os códigos maliciosos podem explorar falhas críticas não documentadas existentes em programas instalados, falhas características de softwares desatualizados ou do firewall, para abrir portas do roteador. Alguns backdoors podem ser explorados por sites maliciosos, através de vulnerabilidades existentes nos navegadores. As falhas podem garantir acesso completo ou parcial ao sistema por um cracker, sendo utilizadas para a instalação de outros malwares ou para o roubo de dados.

- Worms são programas que fazem cópias de si mesmos em diferentes lugares em um computador. O objetivo desse tipo de malware é geralmente saturar computadores e redes, impedindo que eles sejam usados. Ao contrário dos vírus, os worms não infectam arquivos. Uma distinção importante entre vírus e worms de computador é que o vírus precisa de um programa host ativo ou de um sistema operacional ativo já infectado para ser executado, causar danos e infectar outros documentos ou arquivos executáveis, enquanto os worms são programas maliciosos autônomos que se replicam e se propagam por redes de computadores, sem a ajuda das pessoas.

- Phishing é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e

número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.



➔ O spyware compreende uma área meio obscura, pois não existe uma definição oficial para o termo. Como o nome sugere, o spyware é definido de maneira geral e imprecisa como um software destinado a coletar dados de um computador ou outro dispositivo, e encaminhá-los a terceiros sem o consentimento ou o conhecimento do usuário. Muitas vezes, envolve a coleta de dados confidenciais, como senhas, PINs e números de cartões de crédito, o monitoramento de pressionamentos de teclas, o rastreamento de hábitos de navegação e a coleta de endereços de e-mail. Além de tudo isso, essas atividades também afetam o desempenho da rede, deixando o sistema lento e influenciando todo o processo corporativo. Ele costuma ser classificado em quatro categorias principais: cavalos de Troia, adware, cookies de rastreamento e monitores de sistemas.

Para saber mais informações sobre golpes na internet e malwares visite https://cartilha.cert.br/golpes/

2.2 Senha

Pense em sua senha como pensa em uma escova de dentes. Ela é pessoal, você não deixa ninguém usar, e a troca periodicamente por outra de boa qualidade, não é mesmo?

Evite usar números e letras sequenciais, como por exemplo, 1234 ou abcd;

Utilize uma senha diferente para cada conta, em vez de uma única senha padrão;

Não utilize como senha seu nome, ou o de seus filhos e parentes, nem sua

data de nascimento. Senhas que utilizam letras maiúsculas e minúsculas, números e caracteres especiais, como $ & # @ são fortemente recomendáveis..

Sempre desconfie de promoções fáceis e atrativas demais quando for comprar pela Internet. Existem sítios criados apenas para praticar fraudes. Na dúvida, ligue para o telefone informado, verifique o Cadastro Nacional da Pessoa Jurídica (CNPJ) na Receita Federal e faça uma pesquisa sobre a empresa nos sítios de busca e em órgãos de defesa do consumidor;

• Cuidado com e-mails e mensagens no celular que parecem ser de seu banco, do governo, da polícia ou do Poder Judiciário. Geralmente órgãos oficiais e instituições bancárias não usam comunicação eletrônica. Pode ser um golpe. Não forneça seus dados a ninguém e não abra os arquivos que possam vir anexados à mensagem. Na dúvida, consulte diretamente os sítios oficiais ou telefone para obter mais informações;

• Sempre desconfie de e-mails enviados por pessoas que você não conhece. Nunca clique em links ou abra arquivos anexados nas mensagens;

3 SPAM[5]

Spam[6] é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial E-mail).

O spam em alguns pontos se assemelha a outras formas de propaganda, como a carta colocada na caixa de correio, o panfleto recebido na esquina e a ligação telefônica ofertando produtos. Porém, o que o difere é justamente o que o torna tão atraente e motivante para quem o envia (spammer): ao passo que nas demais formas o remetente precisa fazer algum tipo de investimento, o spammer necessita investir muito pouco, ou até mesmo nada, para alcançar os mesmos objetivos e em uma escala muito maior.

5 Texto extraído de https://cartilha.cert.br/spam/

6 Para mais detalhes acesse o *site* Antispam.br, **http://www.antispam.br/**, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), que constitui uma fonte de referência sobre o *spam* e tem o compromisso de informar usuários e administradores de redes sobre as implicações destas mensagens e as formas de proteção e de combate existentes.

Desde o primeiro spam registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias. Atualmente, o envio de spam é uma prática que causa preocupação, tanto pelo aumento desenfreado do volume de mensagens na rede, como pela natureza e pelos objetivos destas mensagens.

3.1 Problemas causados pelo SPAM

Independente do tipo de acesso à Internet usado, é o destinatário do spam quem paga pelo envio da mensagem. Os provedores, para tentar minimizar os problemas, provisionam mais recursos computacionais e os custos derivados acabam sendo transferidos e incorporados ao valor mensal que os usuários pagam.O spam pode afetar os usuários do serviço de correio eletrônico de diversas formas. Alguns exemplos a seguir mostram como a produtividade, a segurança, entre outros, podem ser ameaçadas.

➔ **Não recebimento de e-mails:** Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de spams recebidos seja grande, ele corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, passará a não receber e-mails e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. Outro problema é quando o usuário deixa de receber e-mails nos casos em que regras anti-spam ineficientes são utilizadas, por exemplo, classificando como spam mensagens legítimas.

➔ **Gasto desnecessário de tempo:** Para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal.

➔ **Aumento de custos:** Independente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à Internet, cada spam representa alguns segundos a mais de ligação que ele estará pagando.

➔ **Perda de produtividade:** Para quem usa o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem apagadas por engano ou lidas com atraso.

➔ **Conteúdo impróprio ou ofensivo:** Como a maior parte dos spams é enviada para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

➔ **Prejuízos financeiros causados por fraude:** O spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos, projetados para furtar dados pessoais e financeiros. Esse tipo de spam é conhecido como *phishing/scam*. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas nesse tipo de mensagem fraudulenta.

➔ **Impacto na banda**: o volume de tráfego gerado pelos spams faz com que seja necessário aumentar a capacidade dos links de conexão com a Internet.

➔ **Má utilização dos servidores**: boa parte dos recursos dos servidores de e-mail, como tempo de processamento e espaço em disco, são consumidos no tratamento de mensagens não solicitadas.

➔ **Inclusão em listas de bloqueio:** um provedor que tenha usuários envolvidos em casos de envio de spam pode ter a rede incluída em listas de bloqueio, o que pode prejudicar o envio de e-mails por parte dos demais usuários e resultar em perda de clientes.

➔ **Investimento extra em recursos**: os problemas gerados pelos spams fazem com que seja necessário aumentar os investimentos, para a aquisição de equipamentos e sistemas de filtragem e para a contratação de mais técnicos especializados na sua operação.

Os spammers utilizam diversas técnicas para coletar endereços de e-mail, desde a compra de bancos de dados até a produção de suas próprias listas, geradas a partir de:

➔ **Ataques de dicionário:** consistem em formar endereços de e-mail a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.

➔ **Códigos maliciosos**: muitos códigos maliciosos são projetados para varrer o computador infectado em busca de endereços de e-mail que, posteriormente, são repassados para os spammers.

➔ **Harvesting**: consiste em coletar endereços de e-mail por meio de varreduras em páginas Web e arquivos de listas de discussão, entre outros. Para tentar combater esta técnica, muitas páginas Web e listas de discussão apresentam os endereços de forma ofuscada (por exemplo, substituindo o "@" por "(at)" e os pontos pela palavra "dot"). Infelizmente, tais substituições são previstas por vários dos programas que implementam esta técnica.

3.2 Riscos associados ao SPAM

Spams estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

Algumas das formas como você pode ser afetado pelos problemas causados pelos spams são:

- ➔ 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: caso utilize sistemas de filtragem com regras antispam ineficientes, você corre o risco de ter mensagens legítimas classificadas como spam e que, de acordo com as suas configurações, podem ser apagadas, movidas para quarentena ou redirecionadas para outras pastas de e-mail.

3.3 SPAMMER

Após efetuarem a coleta, os spammers procuram confirmar a existência dos endereços de e-mail e, para isto, costumam se utilizar de artifícios, como:

- ➔ Enviar mensagens para os endereços coletados e, com base nas respostas recebidas dos servidores de e-mail, identificar quais endereços são válidos e quais não são;
- ➔ Incluir no spam um suposto mecanismo para a remoção da lista de e-mails, como um link ou um endereço de e-mail (quando o usuário solicita a remoção, na verdade está confirmando para o spammer que aquele endereço de e-mail é válido e realmente utilizado);
- ➔ Incluir no spam uma imagem do tipo Web bug, projetada para monitorar o acesso a uma página Web ou e-mail (quando o usuário abre o spam, o Web bug é acessado e o spammer recebe a confirmação que aquele endereço de e-mail é válido).

3.4 Como evitar ser um SPAMMER

Muitas pessoas, mesmo sem perceber, em algum momento já enviaram uma corrente da sorte, uma lenda urbana ou algo parecido. Para não se tornar um *spammer,* mesmo entre amigos, é importante respeitar as seguintes dicas:

➔Siga as normas da etiqueta (Netiqueta). É recomendado, por exemplo, sempre preencher o campo do **assunto**com uma descrição significativa do conteúdo do e-mail. Dessa forma, o destinatário terá a opção de não abri-lo, caso não seja de seu interesse.

➔Procure informações a respeito dos diversos e-mails que receber. Muitos usuários, por desconhecimento, reiniciam a propagação de lendas urbanas ou boatos.

➔Antes de enviar um e-mail, reflita se o conteúdo será útil ou de interesse do grupo para o qual pretende remetê-lo.

➔Procure refletir antes de repassar e-mails suspeitos, tais como: boatos, lendas urbanas e até mesmo, golpes. Na dúvida, não envie.

➔Respeite o propósito e o formato das listas de discussão e demais fóruns na rede.

➔Não use listas de mala direta ou particulares de amigos de terceiros para enviar propaganda ou quaisquer divulgações pessoais.

➔Se decidir fazer marketing de sua empresa ou negócios na Internet, informe-se antes sobre as melhores práticas para este fim.

Fonte: http://www.antispam.br/

Bibliografia

Fonte: Cartilha de segurança para internet, Fascículo Códigos Maliciosos

https://cgi.br/media/docs/publicacoes/13/internet_com_responsa_60+.pdf

cartilha.cert.br/fasciculos

https://cgi.br/media/docs/publicacoes/13/internet_com_responsa.pdf

https://cartilha.cert.br/fasciculos/

https://www.nic.br/

https://cartilha.cert.br/

http://cetirp.sti.usp.br/wp-content/uploads/sites/47/2016/02/Cartilha_Boas_Praticas-CeTIRP-USP.pdf

https://www.avast.com/pt-br/c-online-threats

https://inkscape.org/pt-br/doc/tutorials/advanced/tutorial-advanced.html

http://abre.ai/furg

ANEXOS

ANEXO 1

1 - Lembrar sempre o humano.

2 - Não ofender ou magoar os sentimentos dos outros.

3 - Nunca publicar nada que não se dissesse pessoalmente.

4 - Manter os mesmos padrões de comportamento que se segue na vida real.

5 - Ser ético.

6 - Respeitar a privacidade dos outros.

7 - Respeitar a lei.

8 - Saber em que local do ciberespaço se está.

9 - Espreitar antes de saltar.

10 - Não desperdiçar o tempo dos outros.

11 - Não “falar sem saber” e tentar sempre fazer sentido.

12 – Ajudar sempre que se puder.

13 - Não abusar do poder.

14 - Ser compreensivo com os erros dos outros.

15 - Procurar manter uma boa imagem para os outros.

16 - Não incomodar os outros com contactos irrelevantes ou indesejados.

17 - Não ignorar nenhum contacto.

18 - Perguntar ao outro por onde prefere ser contactado.

19 - Ler sempre as FAQ - Frequently Asked Questions (Dúvidas Frequentes).

20 - Não promova a pirataria.

21 - Referenciar a origem das fotografias, da informação ou das citações.

22 - Não falar de assuntos privados em público.

23 - Não enviar ou publicar para “todos” sem motivo.

24 - Não promover as “flame wars”.

25 - Não ser um “troll”.

26 - Não alimentar os “trolls”.

27 - Pedir desculpa pelos erros.

28 - Não humilhar/repreender em público.

29 - Não corrigir erros de ortografia ou de gramática.

30 - Verificar sempre a gramática e a ortografia antes de se enviar ou publicar.

31 - Prestar atenção ao conteúdo das mensagens.

32 - Prestar atenção à “forma” das mensagens.

33 - Utilizar apenas o padrão do idioma.

34 - Não escrever só com maiúsculas ou só com minúsculas.

35 - Não usar palavrões ou calão em certos locais.

36 - Não mentir em relação à sua identidade.

37- Usar uma fotografia real e pessoal para a imagem de perfil.

38 - Respeitar o direito ao anonimato.

39 - Não trabalhar demasiado a imagem.

40 - Não exagerar na autopromoção ou publicidade.

41 - Não fazer publicações de teor publicitário ou de promoção em páginas alheias ou através de mensagens diretas.

42 - Não obrigar os outros a promoverem conteúdos

43 - Não adicionar pessoas a grupos sem critério.

44 - Não adicionar amigos só para “fazer número”.

45 - Não identificar alguém numa fotografia sem critério.

46 - Definir o nível de privacidade de fotografias onde apareçam outras pessoas para, no máximo, os amigos.

47 - Ao iniciar uma conversa com alguém, verificar se o momento é conveniente para o outro.

48 - Definir o estado de disponibilidade corretamente.

49 - Avisar o outro sempre que se tenha de abandonar o teclado, ainda que momentaneamente.

50 - Escrever muitas mensagens curtas em vez de textos longos.

51 - Estar sempre recetivo a explicar possíveis abreviaturas.

52 - Aceitar o desrespeito de algumas regras para se promover a rapidez na escrita.

53 - Não impor um esquema de formatação ao outro.

54 - Não pressupor que o outro está a utilizar o mesmo software.

55 - Cada linha de texto deve ter no máximo 65 caracteres.

56 - Usar parágrafos e frases de tamanho apropriado.

57 - As assinaturas automáticas não devem ter mais de 6 linhas com um máximo de 70 caracteres.

58 - Além de um possível logótipo, não usar imagens, gráficos, “ASCII art”, desenhos ou mapas nas assinaturas.

59 - Usar um nível apropriado de “conversa de circunstância”.

60 - Não usar o email para comunicar más notícias.

61 - Não enviar emails possivelmente embaraçosos.

62 - Não usar o email como forma de escapar à interação social.

63 - Rever sempre o conteúdo do email antes do envio.

64 - Usar apropriadamente a possibilidade de definir a prioridade dos emails.

103

65 - Se não for automático, tornar os endereços eletrónicos em “hiperlinks”.

66 - Prestar atenção à utilização de palavras passíveis de identificar o email como spam.

67 - Alterar o “assunto” do email sempre que - e apenas quando - se justifique.

68 - Dizer no “assunto” o suficiente para que o destinatário fique com uma ideia precisa do conteúdo do email.

69 - Não abusar da função “CC” ou “BCC”.

70 - Não usar a função “BCC” sem aviso ou autorização.

71 - Utilizar a função BCC em envios para um grande número de destinatários.

72 - Diferenciar os destinatários entre “Para” e “CC”.

73 - Se o email foi recebido por “BCC”, ter cuidado com a função “Responder a todos”.

74 - Usar os nomes completos juntamente com os endereços de email.

75 - Responder prontamente aos emails.

76 - Não começar uma nova mensagem para responder a um email.

77 - Começar um novo email para abordar um assunto diferente.

78 - Não adicionar mais destinatários a um email sem o conhecimento do autor ou interlocutor.

79 - Não reencaminhar emails privados.

80 - Não escrever depois do texto citado do email anterior.

81 - Desde que não se pretenda adicionar mais nenhum destinatário a um email longo, citar apenas o material necessário para contextualizar a resposta.

82 - Não alterar o texto de emails a reencaminhar.

83 - Programar as “respostas automáticas” apenas para indivíduos.

84 - Não reenviar anexos que o destinatário já possua.

85 - Utilizar, ou manter, as designações “RE” ou “FW” para as respostas ou reencaminhamentos, respetivamente.

86 - Fazer com que o destinatário perceba porque é que um email lhe foi reencaminhado.

87 - Não reencaminhar emails indiscriminadamente.

88 - Usar o mínimo de formatação de texto.

89 - Não enviar anexos desnecessários.

90 - Evitar anexar ficheiros pesados.

91 - Sempre que relevante, comprimir os ficheiros a anexar.

92 - Não ler os emails privados dos outros.

93 - Não usar métodos para obter notificações de quando os destinatários abrem o email enviado.

94 - Tentar não colocar questões estúpidas.

95 - Verificar sempre por questões similares antes de se perguntar.

104

96 - Respeitar o tópico de discussão.

97 - Não publicar mensagens nos tópicos errados.

98 - Criar tópicos diferentes para assuntos distintos.

99 - Indicar uma publicação longa utilizado no assunto o apêndice [long].

100 - Assinalar claramente possíveis spoilers.

101 - Agradecer ao indivíduo, não ao fórum.

102 - Não incomodar com a persistência.

103 - Colocar o texto citado acima da resposta.

104 - Se não se usar uma ferramenta automática para as citações, referenciar sempre de quando e de quem provém o texto citado.

105 - Ler o tópico completo antes de participar.

106 - Não responder apenas para expressar que se concorda.

107 - Seguir o ritmo de publicações e respostas dos outros utilizadores.

108 - Reabrir um tópico apenas se existirem novas informações relevantes ou úteis.

109 - Não responder a perguntas de TPC.

110 - Não participar em “guerras de edição”.

111- Não usar wikis públicos para autopromoção ou marketing.

112 - Tornar as palavras-chave em hiperligações, mesmo que o tópico ainda não exista.

113 - Respeitar os direitos dos utilizadores.

114 - Não praticar o “cyber-squatting”.

115 - Não “espiar” os colaboradores ou candidatos a emprego.

116 - Ter cuidado ao abordar o emprego e/ou o empregador na internet.

117 - Manter os emails institucionais curtos e focados.

118 - No emprego, usar a internet com moderação.

119 - Ter sempre cuidado com a informação pessoal que se fornece ou publica.

120 - Ser sempre cauteloso nos contactos online.

121 - Não mentir sobre a idade.

122 - Utilizar um programa antivírus e uma firewall.

123 - Não abrir anexos “suspeitos”.

124 - Sempre que disponibilizar ficheiros para download, verifique se contêm vírus.

125 - Reporte sempre que encontrar conteúdos ilegais na internet.

126 - Avise previamente quando o conteúdo que disponibilizar for para adultos ou eventualmente ofensivo.

127 - Criar políticas para evitar o phishing.

128 - Reportar imediatamente qualquer tentativa de phishing.

105

129 - Não enviar informação confidencial, como o número do cartão de crédito, por métodos inseguros.

130 - Não enviar spam.

131- Não responder a spam.

132 - Nunca participar em “correntes de email”.

133 - Nunca reencaminhar avisos sobre “vírus recentes” ou conselhos das autoridades.

134 - Tomar medidas de proteção contra o spam.

135 - Proteger os endereços de email dos “spambots”.

136 - Não usar anúncios pop-up ou pop-under.

137 - Não usar anúncios gráficos que pareçam interativos.

138- Não usar técnicas desonestas para otimizar os resultados dos motores de busca.

139 - Não “abuse” dos serviços online gratuitos.

140 - Caso se use muito um serviço que dependa de contribuições, deve-se contribuir.

141 - Não fazer uma hiperligação para outra página de forma inapropriada.

142 - Escolher apropriadamente se uma hiperligação abre na própria ou numa nova janela.

143 - Caso não seja possível criar uma hiperligação clicável, utilizar um endereço “encurtado”.

144 - Licitar apenas quando se tenciona prosseguir com a compra.

145 - Verificar as condições de envio e de pagamento antes de se licitar.

146 - Esclarecer qualquer dúvida com o vendedor antes de licitar.

147 – Deixar sempre feedback.

148 - Ser honesto no feedback, mesmo que seja negativo.

149 - Apenas criar um blogue se realmente for necessário.

150 - Publicar novos conteúdos regularmente, ou avisar da esporadicidade.

151 - Não comentar apenas para pedir reciprocidade no “seguir” ou no “gosto”.

152 - Depois de um download através de um “torrent” terminar, continuar a partilhar o ficheiro até atingir o rácio de 1.

153 - Usar a internet como forma de promover a ecologia.