A.S
ALMEIDA SANTOS
ADVOGADOS

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: GSI – Gestão de Segurança na Internet					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	18/08/2023	18/08/2025	Anual	17.21
Nome do arquivo: 17.18_ GSI – Gestão De Segurança Na Internet.Docx					

Sumário

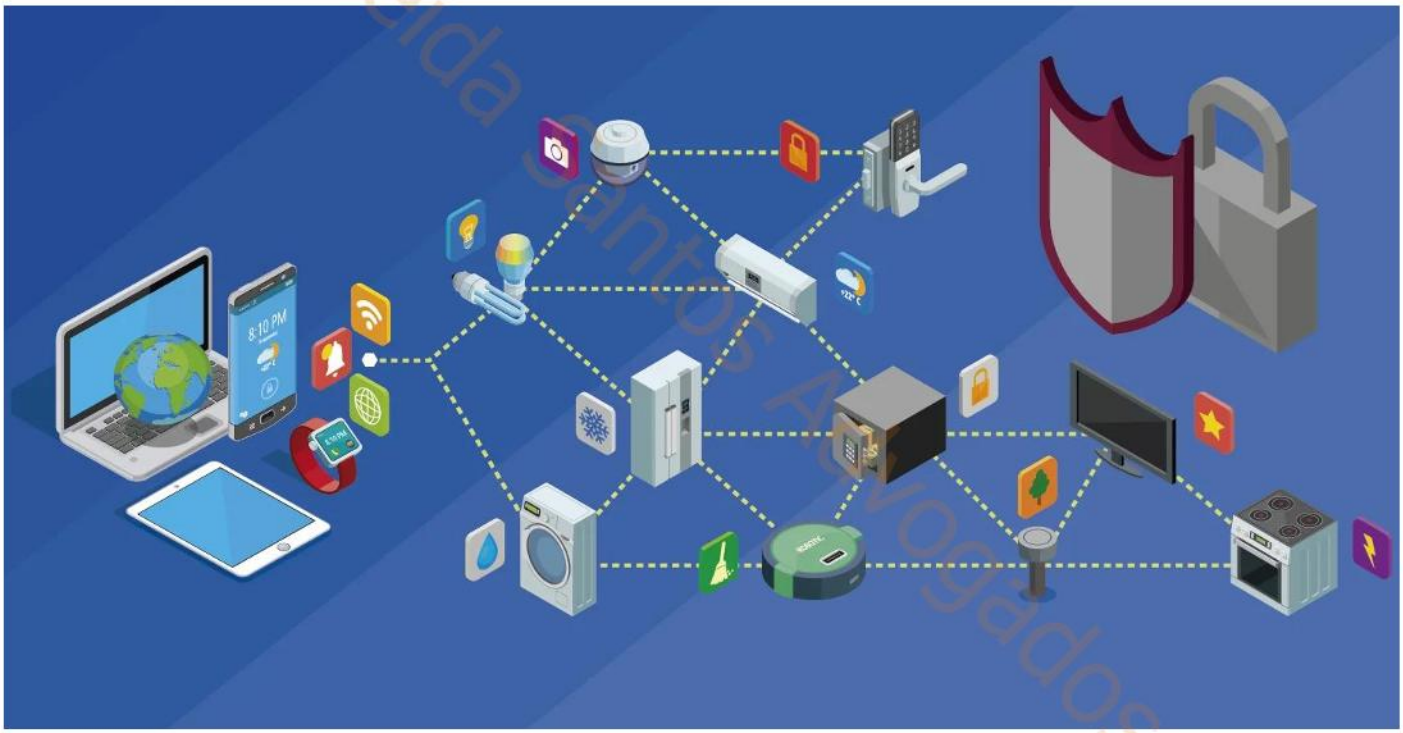
POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: GSI – Gestão de Segurança na Internet					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	18/08/2023	18/08/2025	Anual	17.21
Nome do arquivo: 17.18_ GSI – Gestão De Segurança Na Internet.Docx					

Objetivos

Estabelecer diretrizes que permitam aos colaboradores nas realizações cotidianas a seu trabalho e os riscos a que os usuários estão sujeitos e os cuidados que devem ser tomados.

- Riscos de forma detalhada
- Cuidados a serem tomados e os mecanismos de segurança

Segurança na Internet



A Internet nos trouxe diversos benefícios, viver sem o acesso a ela é praticamente impossível para as empresas, através dela podemos:

- encontrar prestadores de serviços;
- efetuar compras de suprimentos (hardware e software);
- acessar sites para pesquisa de jurisprudencia;
- consultar acervos e obras onde é óssível cnhecer a biografia e as técnicas empregadas;
- declaração de imposto de renda
- entre outros.

Estes são alguns exemplos, para aproveitar esses benefícios de forma segura, requer alguns cuidados seja tomados e para isso é importante conhecer os riscos aos quais estará exposto para que possa tomar as medidas preventivas:

Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar acões em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputacão.

Invasão de privacidade: a divulgacão de informacões pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serção repassadas. Além disto, os sites costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.

Divulgacão de boatos: as informacões na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo. Enquanto isto pode ser desej´avel em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.

Vazamento de Dados

Vazamentos de dados (data leak) ocorrem quando dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros. Com a disseminação dos serviços online, seus dados estão cada vez mais expostos e sendo coletados pelos diferentes serviços disponíveis.

O vazamento pode ser originado:

- do furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas
- do acesso a contas de usuários, por meio de senhas fracas ou vazadas
- da ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros
- do furto de equipamentos que contenham dados sigilosos
- de erros ou negligência de funcionários, como descartar mídias (discos e pen drives) sem os devidos cuidados.
-

Exemplos de dados que podem vazar:

- credenciais de acesso, como nomes de usuário e senhas
- informações financeiras, como números de contas bancárias e de cartões de crédito
- documentos, como CPF, RG e carteira de habilitação

- informações de contato, como endereços e números de telefone
- registros de saúde, como resultados de exames e prontuários médicos
- outros dados, como data de nascimento e nomes de familiares.

Para evitar vazamentos é importante que todos contribuam e você pode ajudar tentando reduzir a quantidade de dados expostos sobre você. Também é importante ficar atento e, no caso de um vazamento envolvendo seus dados, agir rapidamente para reduzir os danos

ATENÇÃO: Após um vazamento é esperado um aumento nas tentativas de golpes por diferentes meios, como e-mails, mensagens de texto e ligações telefônicas.

Riscos Principais

Vazamentos de dados (data leak) ocorrem quando dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros. Com a disseminação dos serviços online, seus dados estão cada vez mais expostos e sendo coletados pelos diferentes serviços disponíveis.

Phishing

Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais. Os fraudadores estão continuamente em busca de novos temas e sistemáticas de captura de novas vítimas. Manter-se bem informado quanto às técnicas, manhas e artimanhas dos cibercriminosos e utilizar softwares anti-phishing, antivírus e firewall são os melhores meios de fugir dessa terrível ameaça.

As múltiplas faces dos fraudadores

Geralmente, os phishers (fraudadores) assumem a identidade de instituições como:

- bancos;
- operadoras de cartão de crédito, telefonia e televisão a cabo;
- provedores de e-mail;
- órgãos do governo (especialmente, a Receita Federal);
- delegacias;
- companhias aéreas;
- lojas virtuais;
- grandes redes varejistas e outras entidades respeitáveis.

Algumas vezes, podem se passar, até mesmo, por pessoas conhecidas da vítima.

Como identificar um ataque Phishing

Em razão da sofisticação dos ataques de phishing, nem sempre é fácil identificar esse tipo de ação criminosa. Prova disso é que, todos os dias, inúmeras pessoas são vítimas de golpistas, das mais diferentes formas e nos mais diversos meios.

No entanto, sempre é possível adotar uma postura preventiva, agindo de forma estratégica para reduzir os riscos de se tornar um alvo de phishing. Para tanto, existem alguns cuidados e boas práticas que devem fazer parte da sua rotina.

Nesse sentido, por exemplo, ao receber mensagens de e-mail ou SMS, é possível checar alguns pontos suspeitos. Caso estejam presentes, há uma grande probabilidade de que se trate de um golpe. Vejamos alguns exemplos:

- recebimento de mensagens não solicitadas;
- mensagens com erros de digitação;
- e-mails desconfigurados, com imagens de baixa qualidade;
- presença de links "soltos".

Além desses pontos objetivos, relacionados à própria estrutura das mensagens, também é importante avaliar o conteúdo daquilo que chega no seu e-mail ou celular. Para isso, a recomendação é:

- conferir o remetente;
- desconfiar de mensagens com propostas "urgentes" e "imperdíveis";
- suspeitar de qualquer mensagem que solicite dados pessoais ou bancários, entre outras medidas.

Códigos maliciosos (Malware)

Código malicioso é um tipo de código de computador ou script da Web nocivo que tem como objetivo criar vulnerabilidades no sistema, gerando backdoors, violações de segurança, roubo de dados e informações, além de outros danos possíveis sistemas de arquivos e computadores. É um tipo de ameaça que o software antivírus pode não conseguir bloquear sozinho. De acordo com a Kaspersky Lab, nem todas as proteções antivírus conseguem lidar com determinadas infecções causadas por código malicioso, que é diferente de malware. Malware se refere especificamente a software malicioso, mas código malicioso inclui scripts de sites que podem explorar vulnerabilidades para fazer upload de malware.

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.

Os principais tipos de códigos maliciosos são:

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu equipamento seja infectado é preciso que um programa já infectado seja executado.

Alguns tipos comnuns:

- **Vírus propagado por e-mail**: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no equipamento.
- **Vírus de script**: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página ou por e-mail, como um arquivo anexo ou como parte do próprio email em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador e do programa leitor de e-mails.
- **Vírus de macro**: tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem, como os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).
- **Vírus de telefone** celular: vírus que se propaga de celular para celular por meio da tecnologia bluetooth ou de mensagens MMS. A infecção ocorre quando um usuário permite o recebimento de um

arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria

Worm

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de equipamento para equipamento. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados nos equipamentos. Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização dos equipamentos.

O processo de propagação e infecção do worm ocorre da seguinte maneira:

- Identificação dos equipamentos alvos: após infectar um equipamento, o worm tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os equipamentos alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras: efetuar varredura na rede e identificar equipamentos ativos; aguardar que outros equipamentos contatem o equipamento infectado; utilizar listas contendo a identificação dos alvos; usar informações contidas no equipamento infectado.
- Envio das cópias: após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes equipamentos, por uma ou mais das seguintes formas: como parte da exploração de vulnerabilidades existentes em programas instalados no equipamento alvo; anexadas a e-mails; via canais de IRC (Internet Relay Chat); via programas de troca de mensagens instantâneas; incluídas em pastas compartilhadas em redes locais ou do tipo P2P (Peer to Peer).
- Ativação das cópias: após realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:
  - imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no equipamento alvo no momento do recebimento da cópia;
  - diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu equipamento;
  - pela realização de uma ação específica do usuário, a qual o worm está condicionado como, por exemplo, a inserção de uma mídia removível.
- Reinício do processo: após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o equipamento que antes era o alvo passa a ser também o equipamento originador dos ataques.

Cavalo de Troia (Trojan)

Cavalo de troia, trojan ou trojan-horse, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Exemplos de trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no equipamento.

Há diferentes tipos de trojans, classificados de acordo com as ações maliciosas que costumam executar ao infectar um equipamento. Alguns destes tipos são:

- ***Trojan Downloader***: instala outros códigos maliciosos, obtidos de sites na Internet.
- ***Trojan Dropper***: instala outros códigos maliciosos, embutidos no próprio código do trojan.
- ***Trojan Backdoor***: inclui backdoors, possibilitando o acesso remoto do atacante ao equipamento.
- ***Trojan DoS***: instala ferramentas de negação de serviço e as utiliza para desferir ataques.
- ***Trojan Destrutivo***: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
- ***Trojan Clicker***: redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
- ***Trojan Proxy***: instala um servidor de proxy, possibilitando que o equipamento seja utilizado para navegação anônima e para envio de spam.
- ***Trojan Spy***: instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
- ***Trojan Banker ou Bancos***: coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy porém com objetivos mais específicos.

Esta classificação baseia-se em coletânea feita sobre os nomes mais comumente usados pelos programas antimalware.

Spyware

pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

- ***Legítimo***: quando instalado em um equipamento pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

- ***Malicioso***: quando executa ações que podem comprometer a privacidade do usuário e a segurança do equipamento, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas spyware são:

- ***Keylogger***: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.
- ***Screenlogger***: similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.
- ***Adware***: projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

Spam

Spam 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 (***U**nsolicited **C**ommercial **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.

Algumas formas que pode lhe afetar 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*.

Prevenção

É muito importante que você saiba como identificar os *spams*, para poder detectá-los mais facilmente e agir adequadamente. As principais características dos *spams* são:

Apresentam cabeçalho suspeito: o cabeçalho do *e-mail* aparece incompleto, por exemplo, os campos de remetente e/ou destinatário aparecem vazios ou com apelidos/nomes genéricos, como "amigo@" e "suporte@".

Apresentam no campo Assunto (*Subject*) palavras com grafia errada ou suspeita: a maioria dos filtros *antispam* utiliza o conteúdo deste campo para barrar *e-mails* com assuntos considerados suspeitos. No entanto, os *spammer* adaptam-se e tentam enganar os filtros colocando neste campo conteúdos enganosos, como ``vi@gra" (em vez de "viagra").

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".

Oferecem opção de remoção da lista de divulgação: 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.

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.

Baseiam-se em leis e regulamentações inexistentes: muitos *spams* tentam embasar o envio em leis e regulamentações brasileiras referentes à prática de *spam* que, até o momento de escrita desta Cartilha, não existem.

Cuidados

Alguns cuidados que você deve tomar para tentar reduzir a quantidade de *spams* recebidos são:

- 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*. É interessante consultar o seu provedor de *e-mail*, ou o administrador de sua rede, para verificar os recursos existentes e como usá-los;

- alguns *Webmails* usam filtros baseados em "tira-teima", onde é exigido do remetente a confirmação do envio (após confirmá-la, ele é incluído em uma lista de remetentes autorizados e, a partir daí, pode enviar *e-mails* livremente). Ao usar esses sistemas, procure autorizar previamente os remetentes desejáveis, incluindo fóruns e listas de discussão, pois nem todos confirmam o envio e, assim, você pode deixar de receber mensagens importantes;
- muitos filtros colocam as mensagens classificadas como *spam* em quarentena. É importante que você, de tempos em tempos, verifique esta pasta, 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 ajudará a treinar o filtro;
- seja cuidadoso ao fornecer seu endereço de *e-mail*. Existem situações em que 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*.

Fonte

- Cartilha de Segurança para a Internet - CERT.br
- https://cartilha.cert.br/spam/