BIM

Boletim Informativo Mensal

Comunicar para Educar

Ano 2 - Nº 18– Julho/2021

Você sabia?

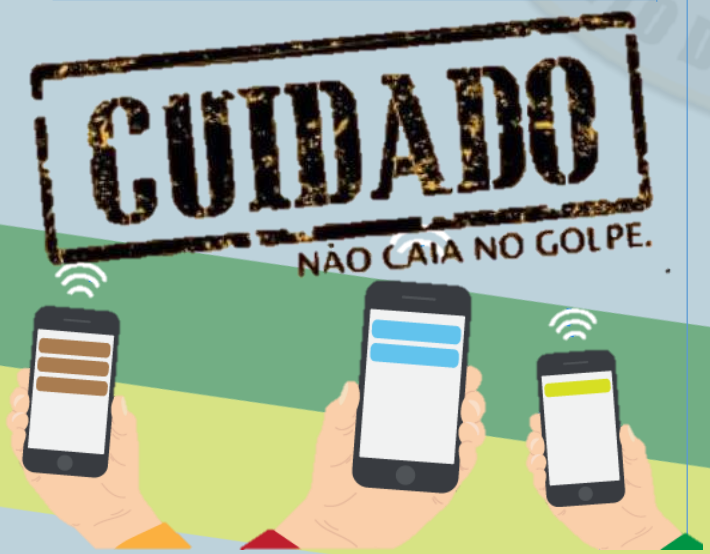
Os responsáveis pelo recebimento do documento com informação classificada em qualquer grau de sigilo, independente do meio e formato, devem:

- registrar o recebimento do documento;
- verificar a integridade do meio de recebimento, e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente; e
- informar ao remetente o recebimento da informação, no prazo mais curto possível.

Além disso, para os casos em que a tramitação de informação classificada ocorra por expediente ou correspondência, o envelope interno somente poderá ser aberto pelo destinatário, seu representante autorizado, ou autoridade hierarquicamente superior.

Mas, se o envelope interno estiver com a marca "PESSOAL", somente poderá ser aberto pelo próprio destinatário.

Para saber mais sobre esse assunto, acesse: http://gov.br/gsi/dsi



Conta falsa, duplicada (estelionato)

Golpe em aplicativo de Mensagem

Um golpe que vem sendo cada vez mais aplicado é a criação de conta falsa, duplicada, nos aplicativos de mensagens. Nessa situação, temos dois possíveis tipos de vítimas: a que teve sua conta duplicada e a que foi extorquida.

Neste crime, o golpista (estelionatário) falsifica o perfil do usuário, utilizando o nome e a foto de perfil original da vítima, só que em outro número. Finge ser a pessoa, e passa a extorquir dinheiro de seus contatos, sem nenhuma interferência na conta real no aplicativo de mensagem desse usuário.

O criminoso conta para cada um daqueles contatos uma estória plausível de troca recente de número; explica a necessidade do envio urgente do dinheiro, por meio de transferência bancária; e tenta convencer essas vítimas a enviar o valor.

Para dar maior veracidade, o golpista utiliza-se de informações reais da vítima, muitas delas disponíveis nos perfis abertos nas redes sociais, como dados pessoais e vínculos de pessoas próximas.

Como se proteger?

1. Mantenha suas contas nas redes sociais como privadas, evite disponibilizar seu número de telefone nessas mídias, bem como a exposição de seus vínculos familiares.
2. Desative a visualização de sua foto de perfil para pessoas que não estão em sua lista de contatos.
3. Desconfie quando alguém conhecido enviar mensagem informando a troca do número de telefone.
4. Entre em contato, imediatamente, com seu conhecido no número de telefone original para verificar se ele realmente mudou de número.
5. Solicite o envio de áudio, faça chamada de vídeo. Observe a escrita, preste atenção no modo com que o outro está digitando; qualquer recusa ou divergência já é motivo para desconfiar.

Uma vez identificado o golpe, denuncie a conta, formalmente, para a plataforma; bloqueie o contato; tire *prints*; reúna comprovantes de pagamento; e faça um Boletim de Ocorrência policial.

Fonte: http://www.gov.br/gsi/dsi https://www.ctir.gov.br/

Editorial/redação/diagramação: ASSESI Sugestões: asscom.dsi@presidencia.gov.br

BIM

Boletim Informativo Mensal

Comunicar para Educar

Ano 2 - Nº 18 – Julho/2021

Aprovada Nova Instrução Normativa do GSI

Com o objetivo de orientar os órgãos e as entidades da administração pública federal (APF) na implementação de processos relacionados à gestão de segurança da informação, publicou-se a Instrução Normativa nº 03 do Gabinete de Segurança Institucional da Presidência da República (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172).

Esse normativo descreve cinco processos de gestão, de realização obrigatória, para os órgãos e as entidades da APF, em conformidade com a Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República:

- mapeamento de ativos de informação;
- gestão de riscos de segurança da informação;
- gestão de continuidade de negócios em segurança da informação;
- gestão de mudanças nos aspectos de segurança da informação; e
- avaliação de conformidade de segurança da informação.

Por meio desses processos, pretende-se que os órgãos e as entidades da APF realizem a Segurança da Informação de forma ainda mais eficaz.

Você, caro internauta, já se perguntou como consegue enviar mensagens, fotos ou vídeos para outros dispositivos eletrônicos?

Para isso, é necessário que esses aparelhos estejam ligados entre si, e que exista uma mesma forma de comunicação.

➢ **E como estabelecer a ligação (conexão) entre dispositivos?**

Há duas formas mais comuns de ligação.

1. Pela chamada “comunicação por fio”, com um cabo de dados ligado em cada dispositivo. Esta é a forma mais comum utilizada em computadores de empresas, ou de órgãos do governo, mas também pode ser utilizada em casa.
2. Conexão por *WIFI,* conhecida como “conexão sem fio”, que utiliza ondas eletromagnéticas. Estas são invisíveis aos nossos olhos e percepções, mas estão ao nosso redor transmitindo mensagens escritas, áudios, fotos ou vídeos.

➢ **E o que é *internet*?**

A *internet* é também conhecida como ”rede mundial de computadores”, que atua no universo cibernético. Neste, imagine uma malha de estradas, avenidas e ruas com muitos endereços. Nestas vias, trafegam os dados de um ponto para outro, todos utilizando a mesma linguagem e seguindo as mesmas regras.

Isso tudo acontece sem você perceber, pois os dispositivos eletrônicos (computadores, celulares, *tablets*, e outros) realizam essa tarefa complexa de forma invisível ao usuário.

➢ **E quem controla, quem é o dono da *internet*?**

Não há um dono. A *internet* é uma rede mundial, onde todos os países conectam suas próprias redes e viabilizam as conexões ao seu povo, interconectando pessoas; cultura; educação; e tecnologia.

Por isso, a segurança da informação, em especial a segurança desse universo cibernético, é tão importante em nossas vidas !!!

Fonte: http://www.gov.br/gsi/dsi https://www.ctir.gov.br/

Editorial/redação/diagramação: ASSESI Sugestões: asscom.dsi@presidencia.gov.br