https://www.ctir.gov.br

18 de junho de 2019

Contato com o **CTIR Gov**

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-2315

Alerta nº 02/2019 – *Recomendações de Segurança da Informação para Integrantes de Órgãos e Entidades de Governo*

Atualização: 27 de junho de 2019

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

1. Sobre o CTIR Gov

O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) faz parte do Departamento de Segurança de Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Entre as competências do DSI[i], destaca-se a de articular, para o estabelecimento de diretrizes para as políticas públicas de Segurança da Informação, com os governos dos Estados, do Distrito Federal e dos Municípios, com a sociedade civil e com órgãos e entidades do governo federal.

O CTIR Gov é um CSIRT de responsabilidade nacional de coordenação e realização de ações destinadas à gestão de incidentes computacionais (monitoramento, tratamento e resposta a incidentes computacionais) em órgãos e entidades governamentais.

O CTIR Gov recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, do presente alerta, contendo orientações de recursos disponibilizados para a prevenção, verificação e mitigação de incidentes relacionados ao tema.

Outros alertas e recomendações podem ser encontrados em *https://www.ctir.gov.br/alertas/*

2. Medidas de Segurança

2.1. Mídias sociais

- Reportar perfis falsos, via Assessoria de Comunicação Social, o ***CTIR.Gov***.
- Evitar divulgar nome completo, telefone, endereço, rotina, localização atual ("*check-ins*"), fotos, viagens e participações em eventos, mantendo o mínimo de informações possíveis em seu perfil de redes sociais.
- Evitar aceitar a amizade ou conversar com desconhecidos na *Internet*.
- Evitar usar *WhatsApp Web*.
- Evitar publicação, comentário ou compartilhamento de informações sensíveis que possam ser usadas em desfavor do usuário.
- Fazer *logoff* sempre que encerrar ou interromper o uso de sistemas, sites ou aplicativos.

2.2. Clonagem ou furto de celular

- O site da Anatel orienta sobre os indícios de um celular ter sido clonado[ii].
- No caso de perda, roubo ou furto do aparelho celular: 1) ligar para a operadora e informar o ocorrido para o bloqueio do *chip*; 2) fazer boletim de ocorrência (serão necessários os números do IMEI e de série do aparelho[iii]).

2.3. Senhas

- Utilizar caracteres alfanuméricos (letras e números) ou biometria para bloqueio / desbloqueio de celular.
- Criar senhas difíceis de serem desvendadas[iv].
- Utilizar autenticação de dois fatores em todas as contas de mídias sociais e serviços de *Internet*, mas nunca por SMS, pois perderá efeito no caso de roubo do celular[v].

2.4. Recebimento de *phishing* (mensagens com *links* maliciosos)

- Em caso de recebimento de *links* suspeitos, seja por *e-mail*, mídias sociais ou SMS, 1) não clicar no *link*; 2) se for o caso, digitar o *link* diretamente no navegador; 3) reportar links suspeitos ao CTIR.Gov[vi].
- Não abrir anexos suspeitos de *e-mail* ou provenientes de instituições, com as quais não se tenha relacionamento.
- Páginas eletrônicas podem ser potenciais armadilhas para ciberataques. Certificar-se de que os dados de bancos ou lojas virtuais são consistentes e se o *site* possui certificação digital (cadeado junto ao endereço da página).
- Evitar fazer o *download* e abrir qualquer arquivo que receber de estranhos. Instituições financeiras não pedem confirmação de senhas e tampouco solicitam dados por *e-mail*, *WhatsApp* ou telefone.
- Cuidado com golpes praticados por *e-mail*, por meio de mensagens com títulos como "Você ganhou" e "Sua conta foi invadida". São mensagens que induzem a vítima a fornecer seus dados (bancários ou outros), preenchendo formulários

em páginas falsas ou, simplesmente, liberando o acesso ao dispositivo, ao clicar em *links* que permitem a instalação de códigos maliciosos no computador ou celular da vítima.

- Não presumir que uma mensagem é legítima com base na confiança que se deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada.

2.5. Recomendações de caráter geral

- Evitar recarregar o celular usando portas USB ou conectar o celular num cabo USB de um desconhecido (havendo urgência, desligue o aparelho antes de carregar).
- Utilizar e manter atualizados mecanismos de segurança como programas *antivírus*.
- Incentivar o fornecimento de treinamento em segurança da informação. O Departamento de Segurança da Informação oferece uma programação anual de treinamentos para os integrantes dos órgãos e entidades de governo.
- Atentar para o conserto ou o descarte de celulares e discos rígidos. Mesmo vazios, seus dados podem ser recuperados.
- Evitar o uso de *webcam* na comunicação com desconhecidos, pois suas imagens podem ser gravadas e alteradas, sem o seu conhecimento. Obstrua a câmera do celular ou do *notebook* quando não estiver em uso.
- Periodicamente: 1) apague as conversas nas mídias sociais e SMS; 2) restaure o celular às configurações de fábrica, instalando o mínimo de aplicativos necessários (cuidado com as permissões de acesso dadas aos aplicativos de celulares).
- Evitar conectar celulares e notebooks a redes públicas de *wifi*.

---

[i] Inciso XI do Artigo 11 do Anexo I ao Decreto Nº 9.668, de 2 de janeiro de 2019.

[ii] Exemplo: dificuldades para completar chamadas originadas; quedas frequentes de ligação; dificuldade para acesso à caixa de mensagem; chamadas recebidas de números desconhecidos, nacional e internacional; e débitos de prestação de serviços muito acima da média.

[iii] Anotar a marca, modelo, IMEI e número de série do aparelho celular, bem como o PIN e PUK do chip quando receber o celular. (Algumas dessas informações constam na caixa do aparelho.)

[iv] Exemplo: evite usar números e letras sequenciais; utilize uma senha diferente para cada conta; não utilize senhas ligadas a dados pessoais ou de familiares; utilize letras maiúsculas e minúsculas, números e caracteres especiais, como $ & # @.

[v] Para saber como, consulte as recomendações “Como agir em caso de perfil falso em Redes Sociais” acessando https://www.ctir.gov.br/alertas/

[vi] Notifique imediatamente a equipe de tratamento de incidentes computacionais, setor de segurança ou suporte de tecnologia da informação da sua organização No caso de não possuir o contato da equipe de segurança de seu órgão, notifique o CTIR Gov, endereço ctir@ctir.gov.br veja como fazer a notificação em: *https://www.ctir.gov.br/arquivos/alertas/2019/recomendacao_2019_01_golpe_phishing.pdf*. Demais formas de contato podem ser verificadas em: *https://www.ctir.gov.br/contato/*.