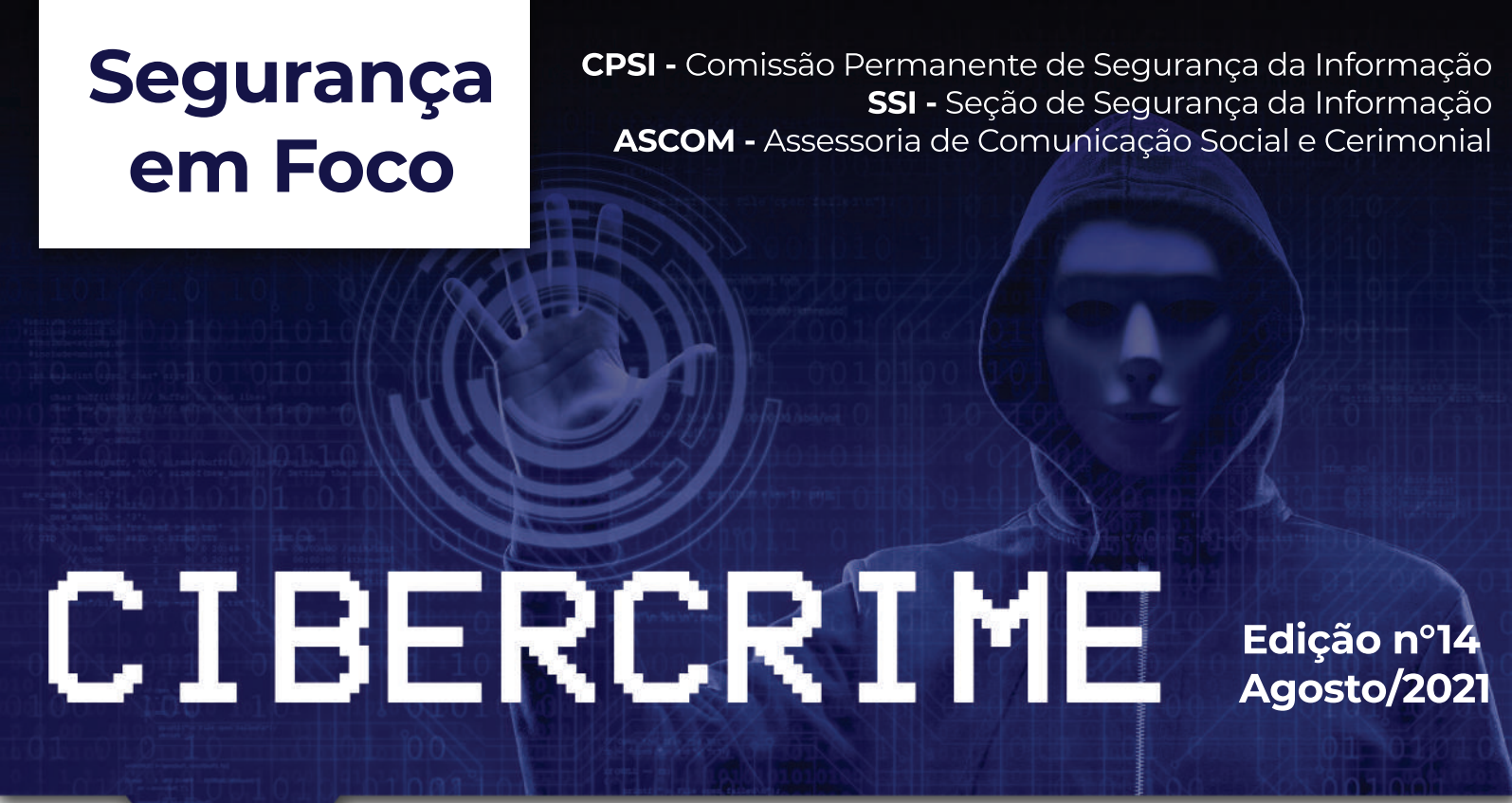
Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial



CIBERCRIME

Edição nº14
Agosto/2021

Cibercrime é o nome dado aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede. Essas práticas podem envolver invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e tantos outros. O cibercrime compreende também os crimes convencionais realizados por meio de dispositivos eletrônicos ou que incluam a utilização de alguma ação digital como instrumento para a prática do crime. Uma das fortes características do cibercrime é a predominância transnacional, o que dificulta as investigações e a apuração de provas contra o acusado. Outra característica também tem relação com o aumento dos computadores pessoais, que permitem que qualquer pessoa no mundo possa realizar práticas criminosas contra indivíduos de qualquer lugar do planeta sem mesmo sair de casa.

O crime cibernético pode ser realizado por aspirantes a *hacker*, organizações criminosas e até organizações patrocinadas por governos. Na maioria dos casos, este tipo de crime visa o lucro. A exceção desses casos são os motivos pessoais ou políticos.

Seguem alguns exemplos específicos de **diferentes tipos de crimes cibernéticos:**

- **Fraude por e-mail e pela Internet;**
- **Fraude de identidades, quando informações pessoais são roubadas e usadas;**
- **Roubo de dados financeiros ou relacionados a pagamento de cartões;**
- **Roubo e venda de dados corporativos;**
- **Extorsão cibernética, que exige dinheiro para impedir o ataque ameaçado;**
- **Interferência em sistemas de modo a comprometer uma rede;**
- **Violação de direitos autorais;**
- **Venda de itens ilegais *on-line*;**
- **Incitação, produção ou posse de pornografia infantil;**
- **Ataques de *ransomware*, um tipo de extorsão cibernética;**
- ***Cryptojacking*, quando *hackers* exploram criptomoedas usando recursos que não possuem;**
- **Espionagem cibernética, quando *hackers* acessam dados do governo ou de uma empresa.**

Agora que já sabemos o que é o crime cibernético, seguem as **principais dicas de como nos proteger:**

- **Mantenha seus *softwares* e o sistema operacional atualizados;**
- **Use *software* antivírus e mantenha-o atualizado;**
- **Use senhas fortes que sejam difíceis de adivinhar e não as registre em lugar algum;**
- **Nunca abra anexos em e-mails de *spam* ou de um remetente que você não conhece;**
- **Não clique em links em e-mails de *spam* ou em sites desconhecidos;**
- **Não forneça suas informações pessoais, a menos que tenha certeza de que é seguro;**
- **Verifique e atualize regularmente as configurações de privacidade em suas contas de mídia social;**
- **Entre em contato diretamente com a empresa para confirmar pedidos suspeitos;**
- **Fique de olho nas URLs em que está clicando. Evite clicar em *links* com URLs estranhas ou que PAREÇAM falsas;**
- **Fique de olho nos seus extratos bancários.**

Por causa da pandemia, surgiu a necessidade das empresas em ofertar serviços de forma cada vez mais remotas e digitais, aumentando assim, o número de ataques cibernéticos, que alcançou índices alarmantes e, em muitos casos, até irreversíveis.

Assim como qualquer crime, dirija-se à delegacia mais próxima e faça um boletim de ocorrência (B.O.). É possível fazer esse registro em qualquer unidade da Polícia Civil, mas se existir em sua cidade, é interessante procurar a Delegacia de Repressão aos Crimes Informáticos (DRCI). É importante guardar tudo o que ajude a provar sobre os crimes que estão ocorrendo. Salve e-mails, dê *'print screen'* (cópia da tela) e preserve as conversas dos aplicativos de mensagens. Com evidências em mãos, é importante registrar uma Ata Notarial no cartório para declarar a veracidade dos documentos e fatos digitais reunidos por você como prova. Esse documento é significativo para que suas evidências sejam registradas como verdadeiras dentro do processo e utilizadas como provas numa futura ação judicial.

Fique ligado: no próximo mês, falaremos sobre *Criptografia*!

Tribunal Regional Eleitoral - RN