CLÍNICA JURÍDICA FPM

CRIMES CIBERNÉTICOS: guia de orientação para micro e pequenas empresas

1 Você sabe o que são Crimes Cibernéticos?

Os Crimes Cibernéticos são atividades ilegais que ocorrem no ambiente digital, utilizando computadores, redes de internet e dispositivos eletrônicos.

2 Vulnerabilidade da Proteção ao Consumidor Empresário

2.1 Qual lei retrata os direitos e deveres do uso da internet no Brasil?

A Lei n.º 12.965/14 que trata sobre direitos e deveres para o uso da internet no Brasil destaca em seu artigo 7º que demonstrando que o acesso a internet é essencial ao exercício da cidadania, ao usuário é assegurado o direito à inviolabilidade da intimidade e da vida privada sua proteção e indenização pelo dano material ou moral decorrente de sua violação.

2.2 Existe alguma lei que tenha objetivo de punir violação de dispositivo informático?

Sim, a Lei Complementar n.º 14.155/21 alterou o crime de invasão de dispositivo informático, melhorando sua redação e aumentando substancialmente suas penas. No art. 154-A do código penal trata de questões relacionadas a crimes cibernéticos, descreve delitos de invasão de dispositivos informáticos, fraudes eletrônicas e estelionatos, entre outros.

2.3 Casos em que houve a ausência de proteção ao consumidor.

Existem casos exemplares que ilustram diferentes situações. Por exemplo, na Apelação Cível 1.0000.20.447353-2/001, uma consumidora foi vítima de uma fraude virtual, onde a empresa cujo site foi falsificado não foi responsabilizada pelos danos devido à cláusula de exclusão de responsabilidade do art. 14, §3º, II do código do consumidor. Já na jurisprudência 1.0000.23.161657-4/001, uma vítima de estelionato tentou responsabilizar uma instituição financeira pelo não recebimento das mercadorias compradas online, porém não conseguiu demonstrar negligência direta da instituição no caso.

2.4 Existe conflito quanto a competência de quem vai julgar o crime cibernético?

Sim, há um conflito sobre quem tem autoridade para julgar crimes cibernéticos. Em um caso específico (Apelação Criminal 1.0027.14.000062-4/001), inicialmente a justiça estadual de Minas Gerais assumiu a competência na segunda instância. Contudo, durante o processo, o juiz declarou-se incompetente devido ao crime envolver material pornográfico com crianças ou adolescentes, o que exigiu que o caso fosse transferido para a justiça federal. Isso ilustra a ambiguidade legal, onde o processo teve que ser movido para a segunda instância antes de determinar que o recurso deveria ser feito na esfera federal.

CRIMES CIBERNÉTICOS: Empresas

3 Como agir se sua micro ou pequena empresa for atacada por um crime cibernético?

1. Informe todos os funcionários sobre o ataque e instrua-os a não interagir com sistemas comprometidos, alinhe-se com a equipe de TI ou um especialista em segurança cibernética para determinar os próximos passos.
2. Identifique a origem e o tipo do ataque e determine quais dados e sistemas foram comprometidos, avaliando assim a extensão do dano.
3. Informe as autoridades competentes, como a Polícia Civil (Delegacia de Crimes Cibernéticos) ou a Autoridade Nacional de Proteção de Dados (ANPD).
4. Notifique as seguradoras, se aplicável e clientes e parceiros comerciais, especialmente se seus dados foram comprometidos, seja transparente e forneça informações sobre medidas que estão sendo tomadas para resolver o problema e proteger os dados no futuro.
5. Trabalhe com especialistas em segurança para remover o malware, fechar brechas de segurança e restaurar sistemas a partir de backups.

Seguir esses passos pode ajudar a minimizar os danos, restaurar a confiança e reforçar a segurança contra futuros ataques.

4 Quais os perigos que as micros e pequenas empresas estão correndo ao se expor nas redes sociais?

As Micro e pequenas empresas estão cada vez mais migrando para o mundo digital visando o alcance e o retorno positivo que gera em torno das empresas, no entanto, ficam vulneráveis a toda essa exposição e acabam correndo riscos sem sequer ter conhecimento.

Podem sofrer ataques onde seus dados bancários, clientes, senhas e quaisquer dados confidenciais serão expostos, levando a perda de credibilidade no mercado, rombos financeiros em suas empresas e até mesmo possíveis consequências judiciais.

5 Você sabe a importância da formação e capacitação dos profissionais que atuam nas empresas?

A formação e capacitação dos profissionais são fundamentais para o sucesso das empresas. Eles garantem que os funcionários estejam atualizados com práticas, tecnologias e habilidades necessárias para desempenhar suas funções de maneira eficaz. Assim vai favorecer com aumento da produtividade, a qualidade do trabalho e a satisfação dos clientes, além de promover um ambiente de trabalho mais positivo e engajado.

6 Como melhorar a segurança cibernética das micro e pequenas empresas para evitar o aumento de invasões em dispositivos informáticos e vazamento de dados?

Para melhorar a segurança cibernética das micro e pequenas empresas é essencial uma abordagem abrangente para que todos os tipos de riscos sejam evitados. Investir em treinamentos específicos para os funcionários é um grande avanço, visto que muitas violações de segurança tem início a partir de um erro humano, como por exemplo clicar em links que dão total acesso a um ataque cibernético Manter os computadores da empresa sempre atualizados no que se trata de antivírus e detectores de intrusão também é importante para ajudar a evitar futuros problemas.

7 Como as micro e pequenas empresas podem identificar potenciais vulnerabilidades em sua infraestrutura de TI antes que se tornem alvos de ataques cibernéticos?

As micro e pequenas empresas podem identificar potenciais vulnerabilidades em sua infraestrutura de TI através de: avaliações de segurança periódicas, como testes de penetração e auditoria, mantendo sistemas e software atualizados com os patches mais recentes, implementando soluções de monitoramento de rede para detectar atividades suspeitas, realizando auditorias internas para revisar políticas de segurança e práticas, educando e treinando os funcionários sobre práticas de segurança cibernética, e considerando a contratação de consultores especializados em segurança cibernética, se necessário.

8 Utilizando mecanismos antivírus você poderá ficar mais seguro!

O principal benefício da utilização de um mecanismo de proteção antivírus é a rápida identificação e bloqueio da instalação de programas que podem ameaçar a segurança e

trazer prejuízos aos seus aparelhos, celulares, computadores e tablets.

Existem vários programas e aplicativos antivírus gratuitos que podem te ajudar a garantir uma maior segurança a sua privacidade e proteção dos seus dados. Como por exemplo:

- Avast;
- AVG;
- Microsoft Windows Security;
- Avira Antivirus.

CRIMES CIBERNÉTICOS: Segurança

9 O que é o contrato de seguro contra roubo de dados?

O contrato de seguro contra roubo de dados cibernéticos protege empresas contra perdas financeiras e danos à imagem devido a vazamentos de dados pessoais dos clientes. Ele define responsabilidades mútuas e é essencial ser revisado e adaptado às necessidades de cada empresa, especialmente microempresas, para garantir cobertura adequada diante de potenciais danos, considerando seu menor poder econômico.

10 Não salve suas senhas bancárias em seu telefone empresarial!

Evite liberar o acesso automático às contas bancárias, salvando suas senhas e dados na conta google, uma vez que se seu celular for invadido, facilitará o acesso dos criminosos às suas contas. É recomendável, ainda, que apenas os sócios ou representante legal da empresa, tenham acesso aos dados bancários da empresa, assim trará uma garantia maior de confidencialidade e segurança, visto que, serão os únicos a terem acessos às movimentações bancárias.

11 Desconfie de e-mails, ligações e mensagens

Devido à fácil acesso à internet, criminosos frequentemente tentam aplicar golpes nas redes sociais. Desconfie de ofertas muito boas e descontos altos, pois nem sempre são confiáveis. Criminosos usam essas ofertas para induzir as vítimas a acessar links e roubar seus dados. Não clique em links nem forneça informações sem pesquisar sobre a empresa primeiro. Dicas rápidas de segurança:

- Desligue ligações suspeitas.
- Apague mensagens com links não confiáveis.
- Delete e-mails com promoções duvidosas.

12 COMPRAS ONLINE - Dicas para comprar com segurança e não cair em golpes.

Microempreendedores, por vezes na pressa do dia a dia, acessam links sem verificar, o que é perigoso por expor a sites não confiáveis. Por isso:

- Verifique o link antes de clicar.
- Escolha empresas conhecidas e bem avaliadas.
- Use cartão de crédito para segurança e facilidade de cancelamento.
- Desconfie de descontos muito altos.
- Leia a política de privacidade.
- Consulte os feedbacks dos clientes.

13 Conscientização do perigo e os problemas causados por acessar links não confiáveis.

Prevenir é essencial para a segurança online. Mantenha-se informado e seja cauteloso ao navegar na internet. Antes de acessar um site, verifique sua segurança. Evite sites de contas desconhecidas em redes sociais para evitar boletos falsos. Confirme promoções e descontos em lojas virtuais. Consulte avaliações no Google antes de comprar. Ao cadastrar-se em sites seguros, esteja ciente dos riscos:

- Clonagem de documentos e cartão de crédito.
- Vazamentos de dados e fotos.
- E-mails falsos de bancos, seguidos de golpes econômicos.

14 Tenha cuidado ao abrir o seu próprio MEI! Conheça alguns golpes modernos aplicados por meio do MEI.

Ao efetuar abertura de sua empresa você deve ficar muito atento ao:

- Receber e-mails com falsos boletos para efetuar pagamento com urgência usando bandeira com sua conta bancária. Saiba que para o MEI, não é necessário pagar nada além da anuidade;
- Receber alertas de segurança sobre um possível acesso a sua conta em um mercado de compra com link indicado para já clicar;
- Receber ajuda com registro de marcas “nome fantasia”, ligações para regularização e até mesmo boleto para registro com as falas de que você poderá perder sua patente ou até ser processado;
- Seu cadastro, que é feito somente pelo portal do governo “GOV”, e-mails recebidos devem ser analisados para verificar a veracidade da origem.

Na dúvida procure o seu contador de confiança.

CLÍNICA JURÍDICA FPM, Unidade Shopping, localizada na Rua Major Gote, n. 1901, 2º andar, bairro Centro, Patos de Minas/MG, CEP 38700-207, Telefone: (34) 3818-2399.

FACULDADE PATOS DE MINAS - FPM

CURSO DE DIREITO

Professora Responsável
Dra. Michelle Lucas Cardoso Balbino

Acadêmicos Responsáveis
Douglas da Silva Oliveira
Eduarda Macedo Braga
Ewertton Martins de Oliveira
Giovanna Gabrielle de Oliveira Castro
Jefferson Luis da Silva
Jhéfiny Queiroz Ferreira
Jordana Lara de Abreu Ferreira
Michelle Timoteo Freitas
Tiffani Natalia Landim Santana
Vitória Caroline do Amaral Cruz