Data: 2020/04/02 JORNAL DE NEGOCIOS - PRINCIPAL
Título: Direito penal prevê até oito anos de prisão para cibercriminosos
Tema: Vieira de Almeida & Associados
Periodicidade: Diaria Âmbito: Nacional
Temática: Gestão/Economia/Negócios Imagem: 1/3
Pág.: 1
GRP: 2.0 %
Inv.: 10456.21 €
Tiragem: 9687
Área: 150704 mm2

Lex

Direito penal prevê até oito anos de prisão para cibercriminosos

SUPLEMENTO 18 a 20

Copyright 2009 - 2020 MediaMonitor Lda.

Data: 2020/04/02 JORNAL DE NEGOCIOS - PRINCIPAL
Título: Direito penal prevê até oito anos de prisão para cibercriminosos
Tema: Vieira de Almeida & Associados
Periodicidade: Diaria Âmbito: Nacional
Temática: Gestão/Economia/Negócios Imagem: 2/3
Pág.: 18
GRP: 2.0 %
Inv.: 10456.21 €
Tiragem: 9687
Área: 150704 mm2

DIREITO PENAL FACE À PANDEMIA

Cibercriminosos arriscam até oito anos de prisão

Numa situação de vulnerabilidade como a que se vive devido à pandemia causada pelo novo coronavírus, as fraudes cometidas através da internet podem ter penas superiores e ir até oito anos de prisão.

JOÃO MALTEZ
jmaltez@negocios.pt

As fraudes são as mesmas de sempre, mas desta vez as práticas ilegítimas têm como pano de fundo uma pandemia. Em causa estão as burlas cometidas através da internet para vender remédios milagrosos ou angariar dinheiro solidário que acaba no bolso dos burlões. A lei identifica estas práticas como crime e, segundo especialistas ouvidos pelo Negócios, quem se aproveite de situações de vulnerabilidade para os cometer arrisca um aumento da pena aplicada pela justiça. No caso de burla informática, a pena máxima pode chegar a oito anos de prisão.

Sofia Ribeiro Branco, sócia da VdA e especialista em direito penal, sublinha que "foram já detetadas situações de esquemas fraudulentos relacionados com a crise epidemiológica" que, inclusivamente, justificaram que a Interpol publicasse uma circular alertando para a ocorrência desse tipo de situações.

Neste tipo de casos, tal como adianta a mesma advogada, para tentar recuperar os valores perdidos, o lesado deverá "apresentar participação junto das autoridades nacionais com competência especializada, com a maior brevidade", como a Polícia Judiciária. Isto para que seja possível desencadear os procedimentos que evitem os danos – designadamente nos casos em que estejam em causa pagamentos bancários – quer, numa segunda linha, a apurar a identidade dos responsáveis, explica.

A advogada Leonor Chastre, especialista em propriedade intelectual e proteção de dados, explica ao Negócios que para estas práticas existe um crime tipificado no regime penal português – o artigo 221.º do Código Penal. Está em causa, concretamente, o crime de burla informática e nas comunicações.

Miguel Baltazar

O atual contexto de crise está a ser aproveitado pelos criminosos para burlar cidadãos e empresas.

Estão a ser usados esquemas criminosos a pretexto da covid-19 que atentam contra cidadãos e empresas, revelam as autoridades.

Sofia Ribeiro Branco lembra que "os esquemas fraudulentos que têm ocorrido neste período de pandemia não diferem dos típicos comportamentos criminosos perpetrados através da internet". No essencial, adianta, do ponto de vista das pessoas singulares, "estão em causa crimes de falsidade informática, de acesso ilegítimo ou de burla informática. Em relação às pessoas coletivas, para além destes, importa também considerar o crime de sabotagem informática".

Numa altura em que o país enfrenta uma crise transversal a todas as áreas, estando os cidadãos e as empresas "numa especial situação de vulnerabilidade e fragilidade", Leonor Chastre entende que a gravidade do crime tenderá a ser maior pelo tribunal. "Se o autor se aproveitar da crise epidemiológica para potenciar a sua atividade criminosa, esta será certamente valorada pelo tribunal", sublinha a mesma advogada.

Opinião idêntica é partilhada por Sofia Ribeiro Branco. "Embora esta situação, em si, não seja legalmente considerada para os crimes em causa serem qualificados, a circunstância de existir um aproveitamento da situação de pandemia que, no fundo, significa explorar vulnerabilidades, será ponderada na graduação da medida da pena", conclui a penalista. ■

Copyright 2009 - 2020 MediaMonitor Lda.

Data: 2020/04/02 JORNAL DE NEGOCIOS - PRINCIPAL
Título: Direito penal prevê até oito anos de prisão para cibercriminosos
Tema: Vieira de Almeida & Associados
Periodicidade: Diaria Âmbito: Nacional
Temática: Gestão/Economia/Negócios Imagem: 3/3
Pág.: 19
GRP: 2.0 %
Inv.: 10456.21 €
Tiragem: 9687
Área: 150704 mm2

Os esquemas fraudulentos que têm ocorrido neste período de pandemia não diferem dos típicos comportamentos criminosos perpetrados através da internet.

SOFIA RIBEIRO BRANCO
Sócia da VdA,
especialista em direito penal

Se o autor [do cibercrime] se aproveitar da crise epidemiológica para potenciar a sua atividade criminosa, esta será certamente valorada pelo tribunal.

LEONOR CHASTRE
Advogada especialista
em proteção de dados

TOME NOTA

Autoridades dão dicas para evitar casos de fraude

No atual contexto, a Interpol e a Polícia Judiciária preparam informação que alerta para a cibercriminalidade. Ficam algumas das suas dicas.

ATENÇÃO ÀS MENSAGENS
Para evitar o sucesso dos burlões, a Interpol recomenda que não responda a mensagens ou chamadas suspeitas; que não abra links e anexos em e-mails e mensagens de texto não solicitadas; e que não partilhe os dados do seu cartão bancário ou informações financeiras pessoais.

DOAÇÕES DE RISCO
O alerta é também para que não compre bens online que pareçam estar esgotados em todos os outros lugares; para que não envie dinheiro para alguém que não conhece; e para que não faça doações para instituições de caridade sem verificar a sua autenticidade.

PROTEÇÃO PREVENTIVA
Entre as práticas preventivas quando faz compras online, as autoridades recomendam a instalação de um antivírus em todos os dispositivos ligados à Net; que recorra a passwords fortes e diferentes para e-mail e redes sociais. Deve ainda proteger os dispositivos eletrónicos com passwords, PIN ou informações biométricas.

COMPRAS SEGURAS
Ainda relativamente às compras feitas online, é recomendável que recorra a fornecedores confiáveis; também que pense duas vezes quando surge uma oferta que parece ser demasiado boa para ser verdade; e, por fim, que verifique a sua conta bancária frequentemente face a atividades suspeitas.

Falsas empresas usam internet para lucrar com pandemia de covid

Apresentam-se como empresas que "vendem" máscaras, medicamentos ou produtos de desinfeção contra a covid-19; ou fazem-se passar por representantes de instituições que angariam verbas para doentes infetados. Há quem compre e há quem contribua, mas nem receberá os produtos adquiridos, nem irá ajudar alguém que precise. Num e noutro caso, descritos em avisos da Polícia Judiciária e da Organização Internacional de Polícia Criminal (Interpol), quem lucra são indivíduos ou instituições criminosas.

Mesmo em tempos de pandemia, o cibercrime não para. Segundo informação avançada pela Interpol, entre os ciberataques observados desde o início de fevereiro de 2020 e associados ao tema da covid-19 foram detetadas campanhas de 'phishing', aplicações com software malicioso, esquemas de partilha de emails com falsas campanhas ou mensagens de telemóvel que convidam os destinatários a efetuar testes de despiste.

No caso do chamado 'phishing', os criminosos recorrem a emails, mensagens telefónicas ou às redes sociais para captar dados pessoais das vítimas ou para a infeção dos seus dispositivos software malicioso. Segundo informação das autoridades, fazem-no escondendo-se atrás da imagem de entidades oficiais como a Organização Mundial de Saúde, a UNICEF ou centros de investigação e laboratórios.

Reuters

Polícias criminais lançam alerta contra crimes informáticos.

Outro dos esquemas fraudulentos assenta na divulgação de plataformas digitais ou de aplicações para dispositivos móveis que aparentam divulgar informação em tempo real sobre a pandemia. Por exemplo, mapas dinâmicos do contágio. Contudo, sem saberem, os utilizadores estão a ser orientados para a infeção de equipamentos software malicioso que afeta os computadores, com o propósito de exigir um pagamento em troca.

Entre os esquemas fraudulentos nas redes sociais está a recolha de donativos para falsas compras de material médico e proteção pessoal.

Surgiram também os alegados cidadãos altruístas, que, através de esquemas de fraude digital partilhados por email ou em redes sociais, divulgam iniciativas para a recolha de donativos para falsas campanhas de compra de material médico ou de proteção pessoal, sublinha a Interpol.

Tal como têm sido utilizadas mensagens de telemóvel informando que, de acordo com a lei, estão a ser aplicadas medidas extraordinárias para o combate à covid-19 para a vacinação dos cidadãos. Para tal, bastaria pagar uma determinada quantia indicada na mensagem e efetuar um registo através de uma ligação (link). Os burlões asseguram a posterior devolução do dinheiro, algo que não é verdade. ■ JM

Copyright 2009 - 2020 MediaMonitor Lda.