

MANUAL
PROTEUS
-
PREVENÇÃO
INFORMAÇÃO
E APOIO A
VÍTIMAS
DE FURTO DE
IDENTIDADE
ONLINE

PROTEUS



Co-financiado pelo Programa
Prevenir e Combater a Criminalidade
da União Europeia



Associação Portuguesa de Apoio à Vítima
Apoyo à Vítima

[illegible]

ISBN	Depósito Legal
978-972-8852-69-6	

Telephone	Fax
+351 21 358 79 00	+351 21 887 63 51

Título
Manual Proteus - Prevenção, Informação e Apoio a
Vítimas de Furto de Identidade Online

E-Mail	Website
apav.sede@apav.pt	www.apav.pt

Autor
2015 © APAV
Associação Portuguesa de Apoio à Vítima

APAV
Rua José Estevão, 135 - A
1150-201 Lisboa
Portugal

ÍNDICE

INTRODUÇÃO	5	3.4.2. Na sociedade	36
1. CASOS TÍPICOS	9	3.5. Dificuldades na investigação	37
< Caso 1 >	11	4. QUADRO LEGAL	39
< Caso 2 >	11	4.1. Enquadramento internacional	41
< Caso 3 >	11	4.2. Lei portuguesa	42
< Caso 4 >	12	4.3. O furto de identidade, a lei nacional e a Convenção do Cibercrime	49
< Caso 5 >	12	5. APLICAÇÃO DA LEI NACIONAL AOS CASOS TÍPICOS	51
< Caso 6 >	12	< Caso 1 >	53
< Caso 7 >	13	< Caso 2 >	53
< Caso 8 >	13	< Caso 3 >	53
< Caso 9 >	13	< Caso 4 >	53
< Caso 10 >	14	< Caso 5 >	54
2. ENQUADRAMENTO CONCEPTUAL	15	< Caso 6 >	54
2.1. Cibercrime	17	< Caso 7 >	54
2.1.1. A universalização do uso da internet	17	< Caso 8 >	54
2.1.2. Definições de cibercrime	17	< Caso 9 >	55
2.2. Furto de identidade	19	< Caso 10 >	55
2.2.1. Dificuldade terminológica	19	6. PREVENÇÃO	57
2.2.2. Tentativa de definição	20	6.1. Medidas de prevenção	59
2.3. <i>Modi operandi</i>	21	6.2. Sinais de infeção do computador por <i>malware</i>	64
3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA	27	6.3. Como identificar sinais de furto de identidade	65
3.1. As situações mais comuns de furto de identidade pela Internet	29	7. CONTENÇÃO	67
3.2. O autor do crime e a vítima	30	7.1. Infeção por <i>malware</i>	69
3.3. Factores de risco	32	7.2. Furto de identidade	69
3.4. Impacto do furto de identidade	33	ANEXOS	73
3.4.1. Na vítima	33	Glossário	75
a. FINANCEIRO	33	Contactos de apoio das instituições bancárias associadas à Associação Portuguesa de Bancos	78
b. LEGAL	34		
c. EMOCIONAL	35		
d. IMPACTO NA ROTINA DIÁRIA	36		



INTRODUÇÃO

[illegible]

INTRODUÇÃO

Um estudo abrangendo 13,022 adultos entre os 18 e os 64 anos de 24 países do Mundo, referente ao ano de 2013, estima que existam 378 milhões de vítimas de cibercrime por ano, um milhão por dia e 12 a cada segundo¹.

A percentagem de população online em 21 países do Mundo que é vítima de burlas de identidade levadas a cabo através da Internet e de acesso não autorizado ao *e-mail* varia entre 1 e 17%, enquanto que da população dos mesmos países entre 1 e 5% é vítima dos comuns furto ou roubo².

Estas vítimas encontram-se numa posição de particular fragilidade e desprotecção, tendo em conta que o cibercrime, pelo seu carácter recente, ainda é pouco valorizado e compreendido pela população em geral e os seus efeitos subestimados também na definição e aplicação de medidas ao seu combate por parte das entidades responsáveis.

Os casos de furto de identidade pela Internet podem ser muito complexos, pelo que as vítimas necessitam de apoio individualizado e qualificado para as auxiliar a recuperar dos efeitos do crime. Será, designadamente, necessária ajuda para operar meios informáticos de contenção do cibercrime, que as vítimas poderão não dominar.

O impacto do cibercrime e, concretamente, do furto de identidade levado a cabo através da Internet, cresce todos os dias, e com ele tem tendência a aumentar o número de vítimas que faz queixa às autoridades policiais e que procura assistência, sendo necessário melhorar a resposta a dar e o apoio a prestar.

É desta necessidade que resulta a elaboração deste manual que, focando-se concretamente no furto de identidade pela Internet, visa preparar os técnicos dos serviços de apoio à vítima para compreender este fenómeno e para auxiliar as vítimas de crime a proceder da melhor forma face ao mesmo.

1 Norton Cybercrime Report, 2013.

2 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime – Draft, February 2013, p.3.

1.

CASOS TÍPICOS

[illegible]

1. CASOS TÍPICOS

< Caso 1 >

Josué, funcionário de um banco, conhecendo os dados de acesso ao *homebanking* de Joaquim, vendeu-os a uma organização criminosa que acedeu à conta da vítima e transferiu 6000 euros para um NIB desconhecido.

< Caso 2 >

Joana considera-se uma pessoa informada no que à cibersegurança diz respeito e toma cuidados para proteger o seu computador. Um dia, Joana, impressionada com o aumento do cibercrime em Portugal, resolveu fazer uma pesquisa sobre os melhores anti-vírus disponíveis. Usou para isso um popular motor de busca e encontrou, entre muitas, uma página dúbia que lhe propunha a transferência de um potente antivírus, a qual optou por não aceitar, uma vez que se encontrava alertada para só aceitar a transferência de informação de fontes fidedignas.

Nessa noite, Joana procedeu a alguns pagamentos através da página do seu banco. Passada uma semana, Joana foi verificar o seu saldo e deparou-se com o desaparecimento de uma considerável quantia de dinheiro.

< Caso 3 >

Jandira e os filhos usam o computador e a Internet para fazer pesquisas e enviar *e-mails*.

Porém, no último mês, o computador de Jandira tornou-se tão lento que ela e os seus filhos desistiram de o utilizar. Na passada segunda-feira, Jandira recebeu um *e-mail* assinado pelo *ReidosHackers* que afirmava ter o seu computador sob controlo e que lhe pedia um “resgate” de 600€ para lhe devolver a livre utilização deste.

1. CASOS TÍPICOS

< Caso 4 >

Josefina gostava de trocar *e-mails* com as amigas e com os familiares emigrados em França.

Um dia deparou-se com um *e-mail* do seu banco que lhe pedia que clicasse num link e que posteriormente confirmasse os seus dados, preenchendo um formulário.

Josefina foi buscar os seus documentos e fez imediatamente o que lhe era pedido.

Passado um mês, Josefina foi contactada pelo seu gestor de conta que, intrigado com a transferência de grande parte do dinheiro guardado para um NIB desconhecido, resolveu esclarecer as suas dúvidas com a cliente.

< Caso 5 >

José recebeu um *e-mail*, que então não sabia ser *spam*, em nome do serviço de *webmail* que utilizava e que lhe pedia a actualização da palavra-passe.

Posteriormente, José foi interrogado por alguns dos seus colegas de trabalho e amigos sobre as mensagens de correio electrónico que andavam a receber do seu endereço e em que este lhes pedia ajuda financeira. Nenhum deles acedeu a tais pedidos.

< Caso 6 >

Joel e Jéssica namoraram durante 5 meses, no fim dos quais Jéssica terminou a relação. Joel, furioso, jurou vingança e Jéssica ignorou-o.

Um dia Jéssica chegou de manhã à escola e reparou que todos os seus colegas olhavam para ela, cochichando entre si e rindo. Depois de entrar na sala de aula perguntou à sua colega Jurema se sabia o motivo de tantos risos e esta contou-lhe que existia um perfil na rede social *Facebook*, com o nome de Jéssica e com a sua fotografia de perfil, em que esta apregoava praticar relações sexuais em troca de pequenas somas de dinheiro.

1. CASOS TÍPICOS

< Caso 7 >

Joana, que conhecia o nome completo e a morada de Juliana, criou um *e-mail* com o nome desta e inscreveu-se num site de vendas online com o nome de Juliana, a sua morada e o *e-mail* com o seu nome. Seguidamente, procedeu à publicação de anúncios de venda de *tablets*. João, interessado em adquirir o *tablet*, procedeu ao pagamento e nunca chegou a receber o equipamento. Juliana foi notificada algum tempo depois para ser interrogada como arguida por um crime de burla informática.

< Caso 8 >

Julieta recebeu um telefonema de alguém que dizia ser do “Novo Banco” e que, devido aos recentes acontecimentos, necessitava de confirmar alguns dos seus dados pessoais. Julieta acedeu, aliviada por saber que não tinha ficado ligada ao “Banco Mau”. Dois meses depois, Julieta recebeu uma conta do seu cartão de crédito relativa a compras feitas *online* pelo criminoso.

< Caso 9 >

Foram enviadas mensagens para vários endereços de *e-mail* que aparentavam ser do serviço de *webmail* utilizado e que pediam a actualização da palavra-passe. A mulher de Júlio introduziu os seus dados e, desse modo, o cibercriminoso teve acesso à caixa de entrada desta, ficando a conhecer inúmeros dos seus dados pessoais, assim como da sua família. Júlio foi posteriormente contactado por duas companhias de crédito que pretendiam confirmar se as candidaturas à obtenção de crédito no seu nome eram legítimas. Júlio, que nunca tinha recorrido ao crédito, esclareceu que não se havia candidatado junto de nenhuma das empresas. Ficou abismado com a quantidade de dados pessoais seus que o criminoso conhecia. As candidaturas foram declinadas. Um mês depois, Júlio dirigiu-se ao seu Banco pretendendo contrair um empréstimo para a compra de uma casa. Tal empréstimo foi recusado devido às muitas candidaturas à obtenção de crédito feitas em seu nome nos últimos meses.

1. CASOS TÍPICOS

< Caso 10 >

Jair é vítima de *bullying* desde que entrou na Escola Secundária de Odivelas.

Certo dia, Jair chegou a casa e acedeu ao seu perfil na rede social *Facebook*. O seu coração parou de bater por momentos quando verificou que tinham sido publicadas, com a sua conta, várias fotos suas de roupa interior.

O desespero tomou conta de Jair quando este se lembrou de que a única pessoa que conhecia o seu nome de utilizador e palavra-passe do *Facebook* era Jaime, o seu único amigo.

2.

ENQUADRAMENTO CONCEPTUAL

[illegible]

2. ENQUADRAMENTO CONCEPTUAL

2.1. Cibercrime

2.1.1. A universalização do uso da internet

Em 2011, pelo menos 2,3 mil milhões de pessoas, ou seja, mais de um terço da população mundial, tinha acesso à Internet³. Estima-se que no ano de 2020 existam seis dispositivos em rede por pessoa, o que obviamente indica que, cada vez mais, a criminalidade se “servirá” da Internet.

As tecnologias de informação e comunicação (TIC) constituem novos meios de cometer crimes. A conexão global através da Internet e o uso destas tecnologias viabilizam também o aparecimento de novos tipos legais de crime.

Igualmente, as TIC facilitam a internacionalização da criminalidade, isto é, por exemplo, o autor pode praticar um crime no Brasil contra uma vítima de Portugal, sem qualquer dificuldade, que é o que acontece, geralmente, nos casos de *phishing* como o que é relatado no caso nº 4 neste manual.

O cibercrime tem vindo, assim, a aumentar, sendo praticado quer por organizações criminosas, quer por criminosos a título individual, que procuram novas oportunidades de obtenção de lucros e de outras vantagens, ou que actuam com propósitos relacionados com o foro da intimidade, através de redes sociais, nomeadamente.

2.1.2. Definições de cibercrime

Não existe uma definição consensual e universal de cibercrime. As leis nacionais e internacionais não a consagram e não existe doutrina consolidada sobre o assunto.

As definições de cibercrime, segundo o Departamento de Drogas e Crime da ONU, dependerão do uso que se pretende dar ao termo.

O mesmo Departamento, face aos instrumentos nacionais e internacionais que se abstêm de fornecer uma definição *per se* de cibercrime, procura descrever o conteúdo do termo através de uma enumeração das condutas ou actos que nele se englobam⁴. Lista, assim, não exaustivamente, catorze comportamentos passíveis de constituir cibercrime, divididos em três categorias:

3 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime – Draft, February 2013, p. 1.

4 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime – Draft, February 2013, pp. 11 e 12.

2. ENQUADRAMENTO CONCEPTUAL

Actos contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos	Actos praticados através de computador para obtenção de benefícios pessoais ou financeiros	Actos praticados através de computador para obtenção de benefícios pessoais ou financeiros
> Acesso ilegal a sistema informático; > Acesso ilegal, interceptação ou aquisição de dados informáticos; > Interferência ilegal com sistema ou dados informáticos; > Produção, distribuição ou posse de ferramentas para uso indevido de computador; > Violação de meios de protecção de dados ou privacidade.	> Fraude ou falsidade informática; > Ofensas relacionadas com a identidade praticadas através de computador; > Ofensas relacionadas com direitos de autor e marcas registadas praticadas através de computador; > Envio ou controlo do envio de spam; > Actos praticados através de computador que causam danos pessoais > Solicitação e aliamento de crianças através de computador.	> Incitamento ao ódio através de computador; > Produção, distribuição ou posse de pornografia infantil praticadas através de computador; > Actos de apoio ao terrorismo praticados através de computador.

A Comissão Europeia, na sua comunicação ao Parlamento Europeu, ao Conselho e ao Comité das Regiões - *Rumo a uma política geral de luta contra o cibercrime* – define cibercrime como «os actos criminosos praticados com recurso a redes de comunicação electrónicas e sistemas de informação ou contra este tipo de redes e sistemas».

Parece-nos que a divisão do conceito de cibercrime em conceito amplo e conceito restrito, englobando o primeiro todos os actos criminosos que podem ser levados a cabo por meios informáticos, ainda que estes não sejam mais que instrumentos para a sua prática, não integrando o seu tipo legal, e o segundo só os crimes em que a componente digital aparece como elemento do tipo legal de crime ou mesmo como o seu objecto, é completa e clara⁵.

5 Ver Dias Venâncio, Pedro, *Lei do Cibercrime - Anotada e comentada*, Coimbra Editora, 2011, p.17.

2. ENQUADRAMENTO CONCEPTUAL

2.2. Furto de Identidade

2.2.1. Dificuldade terminológica

Existe muita polémica em torno do termo “identidade” e, por isso, refere-se desde já que, no contexto deste manual, o termo referir-se-á a todos os dados relativos a uma pessoa cujo uso por outra pessoa lhe permita fazer-se passar pela primeira em ordem à prática de actos criminosos.

O termo “furto de identidade”, apesar de ser o escolhido para ser utilizado neste manual, não define com correcção o fenómeno a que pretende referir-se.

Na verdade, nenhum dos termos que habitualmente são usados neste contexto, por influência das expressões utilizadas na língua inglesa – “furto de identidade”, “roubo de identidade”, “fraude de identidade” – goza de correcção terminológica.

Com efeito, os casos com que vamos deparar-nos implicam que o criminoso obtenha os dados pessoais ou certas palavras-passe ou códigos pessoais da vítima e os utilize para praticar crimes.

Não poderá falar-se de furto ou de roubo, uma vez que a subtracção de bens móveis a que se refere o Código Penal (CP), nos artigos 203º e 210º, não abrange obtenção de dados ou palavras-passe.

Também não deverá falar-se de fraude, uma vez que este termo não tem consagração jurídica no ordenamento português.

No que à língua inglesa diz respeito, os termos “*identity theft*” e “*identity fraud*” parecem ser utilizados, na maioria dos casos, com o mesmo significado, sendo “*identity theft*” mais utilizado nos Estados Unidos da América e tendo “*identity fraud*” uma maior aplicação no Reino Unido. Neste último Estado, porém, procurou delimitar-se o sentido de cada um dos termos⁶.

Opta-se, neste manual, pela expressão “furto de identidade” para designar o fenómeno em apreciação, tendo em conta que nos parece ser de excluir a possibilidade de usar a designação “fraude de identidade”, tendo em conta a sua falta de conteúdo jurídico, e a expressão “roubo de identidade”, por não haver geralmente qualquer violência ou constrangimento associados às condutas que compõem o fenómeno em foco.

6 *Identity theft* ou furto de identidade é a obtenção dos dados identificativos de outrem sem o seu conhecimento ou consentimento e *identity fraud* ou fraude de identidade é o uso da identidade de outrem, em actividade criminosa, para obter bens ou serviços através do engano; cfr. James Jones, *Understanding ID fraud and how to stop it*, *The Anonymous Attacker*, CIFAS, 2009, p.6. Ambos os sentidos mencionados são englobados na noção aqui utilizada de furto de identidade pela Internet.

2. ENQUADRAMENTO CONCEPTUAL

Assim, “furto de identidade” ainda que não constitua uma designação precisa, parece ser a que tem uma maior correspondência com os comportamentos que se pretendem definir e estudar.

2.2.2. Tentativa de definição

Decorre de tudo o que acima se disse que, tal como no caso do cibercrime, não existe uma definição uniforme de furto de identidade. Procuraremos definir quais os actos que entendemos encontrar-se englobados por este fenómeno, para o efeito de construção deste manual.

Começemos por deixar claro que, em Portugal, o furto de identidade não é um tipo legal de crime, mas sim um fenómeno a que se aplicam vários tipos legais de crime.

Segundo a *Federal Trade Commission* dos EUA, «o furto de identidade ocorre quando alguém usa a informação pessoal de outrem sem o seu consentimento para cometer fraude ou outros crimes⁷».

Segundo o *Fraud Prevention Expert Group* da Comissão Europeia, o núcleo do fenómeno, que se retira das definições fornecidas para *identity theft* e *identity fraud*, é a apropriação e uso dos dados identificativos de alguém para levar a cabo actividades ilegais.

Já de acordo com a Divisão de Crime Económico do Conselho da Europa, o termo “furto de identidade” descreve os actos em que o perpetrador obtém e usa enganosamente a identidade de outrem. Estes actos podem ser praticados sem a ajuda de meios técnicos, mas também podem fazer uso de tecnologia informática.

Algumas definições, que variam de país para país, centram-se mais no acto de obter os dados, enquanto outras exigem o propósito de, com a obtenção de tais dados, praticar determinados actos ilícitos.

O elemento comum às várias definições que vão sendo propostas é que a conduta descrita diz respeito a uma ou mais de três fases – a fase da obtenção de dados pessoais, a fase de possuir ou transferir os dados (sabendo que estes serão utilizados para a comissão de um crime) e, finalmente, a fase de utilização dos dados para a prática de crimes.

Procurando chegar a uma definição o mais ampla possível, pode dizer-se que o furto de identidade abrange a obtenção não consentida dos dados pessoais e/ou secretos da vítima, a sua

7 Esta definição é utilizada no manual de atendimento a vítimas de crime do serviço de apoio à vítima do Departamento de Justiça dos EUA.

2. ENQUADRAMENTO CONCEPTUAL

posse ou transferência, com consciência de que serão utilizados para fins criminosos e a sua utilização para a prática de crimes.

Referindo-se este manual ao furto de identidade pela Internet, os actos serão abrangidos pela definição do fenómeno, quer os dados pessoais da vítima sejam obtidos via Internet (como nos casos 2 e 4), quer os dados sejam obtidos por outro meio mas transferidos através da Internet ou usados para cometer um crime pela Internet (como nos casos 1, 8 e 10). Caso o crime se consubstancie apenas numa das fases, a conduta a ela correspondente – obtenção, posse ou utilização - tem que ser praticada através da Internet, para caber no conceito em foco.

Como se referiu, uma vez obtidos os dados da vítima, o criminoso pode utilizá-los para praticar crimes. Esses crimes serão de três tipos: crimes não relacionados directamente com a vítima mas praticados em seu nome (como nos casos 5 e 7), crimes que visam o enriquecimento do autor do crime ou de um terceiro e que causam danos directos à vítima (como nos casos 1, 2, 4, 8 e 9) e crimes que visam a difamação da vítima (como nos casos 6 e 10).

2.3. *Modi operandi*

A obtenção dos dados da vítima pode ser levada a cabo por uma série de meios, que tendem a multiplicar-se e diversificar-se. Neste âmbito, a inovação, visando “despistar” quer os mecanismos de detecção dos utilizadores, quer a actuação das autoridades, é constante. Por este motivo, a abordagem aos vários meios terá que ser genérica, para não ficar rapidamente desactualizada.

Existem métodos mais tradicionais de conseguir as informações pessoais de alguém, como o de vasculhar no lixo, interceptar correio, furtar certos documentos identificativos ou outros documentos ou relatórios que contenham informação pessoal ou financeira da vítima, fazer-se passar por senhorio, potencial empregador ou outra pessoa que pudesse pedir este tipo de documentos, procurar obter informações junto a pessoas próximas da vítima, contactar a vítima ou os bancos com falsos pretextos para obter informações privilegiadas (ver caso 8), comprar estas informações ou ainda observar a vítima enquanto ela utiliza a informação a obter (imagine-se, por exemplo, a situação em que um colega de trabalho da vítima observa-a a introduzir os dados de acesso à sua conta para depois os utilizar com o intuito de retirar dinheiro da mesma).

Todos estes meios poderão estar compreendidos no conceito de furto de identidade pela Inter-

2. ENQUADRAMENTO CONCEPTUAL

net, nos termos em que o definimos, uma vez que a informação obtida por meios não informáticos pode ser utilizada para praticar um qualquer crime através da Internet.

Outro método de obtenção de dados da vítima, físico mas não tradicional, é o furto de *hardware* ou do telemóvel contendo informações pessoais ou secretas da vítima.

Vistos os principais métodos tradicionais, analisemos os métodos que fazem uso das novas tecnologias, mais concretamente, da Internet.

As comumente denominadas “Cartas da Nigéria” que, inicialmente, surgiam sob a forma de cartas, telex e fax e actualmente consistem, muitas vezes, em mensagens de correio electrónico, constituem um meio de comissão de burla de identidade, que tanto recorre aos meios tradicionais de obtenção de dados como à Internet.

A correspondência vem, geralmente, redigida em inglês, quase sempre deficiente, e era tradicionalmente dirigida a pessoas com posições importantes no meio empresarial, na administração pública, na política e noutros sectores influentes da sociedade. Hoje, contudo, o destinatário pode ser qualquer pessoa. O remetente identifica-se como pertencendo ao alto quadro do governo ou de uma companhia estatal de determinado país africano, ou como sendo familiar de alguém que pertence.

Nos primeiros anos, o país emissor era quase sempre a Nigéria. Depois, alargou-se a alguns países geograficamente próximos deste e ultimamente também já da África do Sul chega este tipo de correspondência.

A mensagem consiste numa proposta de negócio. O remetente diz possuir uma elevada quantia de dinheiro conseguida devido ao seu estatuto privilegiado, relacionado com a administração do seu país.

Dizendo não poder ser associado publicamente a essa fortuna, em razão da origem, justifica a necessidade de a transferir para o estrangeiro. Pede assim ao destinatário que receba numa sua conta bancária esse dinheiro, a troco de uma percentagem desse valor. Para tal, o remetente pede o envio dos dados identificativos dessa conta, os seus dados pessoais, da sua empresa ou organização incluindo papel timbrado, etc.

Nem sempre todos estes elementos são pedidos na primeira carta ou *e-mail*, mas sim nos seguintes, quando o destinatário responde e permite, assim, o diálogo.

2. ENQUADRAMENTO CONCEPTUAL

Com os dados das pessoas físicas, das pessoas colectivas e das contas bancárias, os criminosos podem cometer burlas à escala internacional (o que ocasionalmente acontece), mediante a utilização fraudulenta dessa informação no sistema financeiro.

Outro processo de obtenção de dados passa pela publicação em jornais ou na Internet de falsos anúncios de emprego, que visam chamar a atenção das vítimas de modo a obter os seus dados para proceder a furto de identidade e burla. Estes são os chamados *job scams* que, igualmente, fazem uso dos meios tradicionais de obtenção de dados ou da Internet.

Importa também atentar nos pedidos de ajuda enviados através do *e-mail* ou do *Facebook* de outrem para amigos ou conhecidos deste. O *phishing* para obtenção de acesso ao correio electrónico de alguém serve em muitos casos exactamente para atribuir credibilidade a estes pedidos de ajuda – veja-se o caso 5 apresentado. Com o mesmo objectivo, procede-se ao acesso à conta de *Facebook* das vítimas de furto de identidade, podendo os pedidos de ajuda ser publicados na página de perfil ou ser enviados através de mensagens privadas.

O *Facebook* pode servir também para obter os dados de novas vítimas de furto de identidade. Através da introdução de *malware* nos computadores, são publicados nas páginas de *Facebook* das vítimas *links* que visarão obter dados de outros utilizadores. Assim, por exemplo, é publicado um vídeo na página de uma vítima para que os amigos desta, ao clicarem em “gosto” do vídeo, sejam encaminhados para uma página que lhes solicita a introdução dos seus dados pessoais.

Também os motores de busca, como o Google, que permitem a pesquisa de milhões de páginas em segundos, podem ser utilizados com fins ilícitos. *Google hacking* é um termo utilizado para descrever complexas consultas nestes motores de busca, que têm como fim encontrar alvos desprotegidos e dados sensíveis em *websites*. A *Google Hacking Database* facilita esta tarefa. É uma base de dados de consultas que identifica dados sensíveis. A *Google Hacking Database* identifica avisos e vulnerabilidades do servidor, as mensagens de erro, que contêm muita informação, ficheiros com senhas, directórios sensíveis, páginas que contêm portais de *log-on*, páginas que contêm dados de rede ou de vulnerabilidade, como *logs* de *firewall* e embora a *Google* procure bloquear as investidas dos *hackers*, nada os impede de se infiltrar nos *websites* e de proceder às consultas da *Google Hacking Database*.

Outra situação é a de funcionários (ou alguém fazendo-se passar por estes) que, tendo acesso à informação identificativa e secreta da empresa em que trabalham, dos membros da gerência

2. ENQUADRAMENTO CONCEPTUAL

e administração, de outros funcionários ou de clientes da empresa, obtêm estes dados com intuios criminosos, pretendendo, muitas vezes, vender a informação, maioritariamente a organizações criminosas (veja-se o caso 1).

Um dos métodos de obtenção de dados pessoais para furto de identidade mais comuns e que tem recebido muita atenção por parte das autoridades e dos *media* é o chamado *phishing*. Esta actividade traduz-se no envio em massa de mensagens de correio electrónico (*spamming*), que contém um *link* para uma página na *web*. Esta página é, normalmente, uma reprodução aproximada de uma outra de um banco ou de uma entidade emissora de crédito, por exemplo, e contém elementos identificadores da entidade autêntica e imagens a ela referentes. No entanto, será uma página falsa. Se a vítima usar o *link* para aceder à página falsa, ser-lhe-á pedido que se identifique, introduzindo os seus códigos confidenciais, referentes à sua conta bancária ou ao seu cartão. A captura, por esta via, destes dados permitirá ao criador da página aceder às contas bancárias das vítimas e transferir o dinheiro que aí houver para outra conta ou utilizar o cartão de crédito em seu proveito.⁸ O caso 4 pretende representar um exemplo clássico da ocorrência deste fenómeno.

No *phishing* poderão, então, ser identificadas quatro fases: a fase inicial consiste na remessa massiva de mensagens de correio electrónico com um *link* para uma página *web*; na segunda fase, a vítima, sem o saber, dá a sua informação pessoal/palavras-passe/códigos de acesso ao autor do crime - este momento consistirá, na maioria das vezes, na introdução dos dados pessoais da vítima no *site* falso; na terceira fase, o autor do crime entra na verdadeira página da instituição bancária, introduz os dados da vítima e retira dinheiro da conta; a quarta fase consiste no branqueamento de capitais, processo pelo qual os autores de algumas actividades criminosas encobrem a origem dos bens e rendimentos (vantagens) obtidos ilicitamente, transformando a liquidez proveniente dessas actividades em capitais reutilizáveis legalmente, por dissimulação da origem ou do verdadeiro proprietário dos fundos.

Falando dos novos métodos de obtenção de dados privados para cometer furto de identidade, atente-se ainda no *pharming*, que se trata de uma «*técnica que utiliza os métodos de difusão de vírus que têm formato de verme – os worms. Passa pela difusão, por via de spam – portanto de correio electrónico -, de ficheiros ocultos que, igualmente de forma oculta, se auto-instalam nos computadores ou sistemas informáticos das vítimas. Uma vez alojados, estes ficheiros alteram de forma oculta, sem o conhecimento do dono do computador, os arquivos do sistema, designadamente os ficheiros contendo os populares “favoritos” e o registo de cookies. Por via desta alteração, quando o dono do computador acede ao seu habitual site bancário, o sistema,*

8 Cfr. Pedro Verdelho, *Phishing e outras formas de defraudação nas redes de comunicação*, Direito da Sociedade de Informação, Vol. VIII, p. 417.



2. ENQUADRAMENTO CONCEPTUAL



ardilosamente alterado, redirige-o para um outro site, construído e disponibilizado online com métodos idênticos ao do phishing.⁹»

Outra técnica que importará referir neste âmbito é o *sniffing*, que consiste na captura de informações enviadas para outros computadores. Os computadores em rede partilham canais de comunicação, sendo que, nos canais partilhados, os computadores podem receber informações enviadas a outros computadores.

Finalmente, refiramos o *hacking* e o *cracking*, ambos formas de aceder ilicitamente a sistemas informáticos e, portanto, também meios de obtenção de informações privadas. Neste contexto, ambos os termos se referem ao acto de quebrar códigos de segurança ou de obter ilicitamente códigos de licença de programas para ter acesso, sem autorização, ao computador alheio. O caso 3 descreve uma situação em que um *hacker* acedeu ao computador de Jandira e obteve controlo sobre o mesmo, tornando-o inutilizável, para posteriormente pedir um resgate, ou seja, um montante para resolver o problema que causou. Não estamos, neste caso, perante furto de identidade através da Internet, a não ser que o *hacker* tenha obtido os dados de Jandira através do acesso ao seu computador.

Data mining consiste em analisar dados, procurando criar padrões e estabelecer relações entre estes. Esta técnica é utilizada em muitas áreas de pesquisa. Existem programas de computador, os chamados *data miners*, que recolhem informação disponível na Internet ou nos computadores das vítimas sem a sua autorização, a analisam e criam padrões. Isto permite, por exemplo, às empresas prever o comportamento dos consumidores e, no que diz respeito ao furto de identidade, viabiliza a organização dos dados identificativos da vítima, para que estes possam ser utilizados pelo cibercriminoso.

Atentemos, finalmente, no *keylogging*, que consiste na utilização de um programa de computador que, quando instalado no mesmo, permite registar tudo o que é digitado no teclado. Este método ludibria os cibernautas mais cuidadosos, como Joana, a protagonista do caso 2. Pode bastar a abertura de uma página da *web* para que se dê a instalação de *malware* no computador, não sendo necessário proceder a uma transferência de dados. Neste caso foi instalado um programa de *keylogging* que permitiu ao criminoso captar tudo o que foi introduzido no teclado, inclusivamente os códigos de acesso à página do banco.

9 Pedro Verdelho, *Phishing e outras formas de defraudação nas redes de comunicação*, Direito da Sociedade de Informação, Vol. VIII, pp. 415 e 416.



3.

FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

[illegible]

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

3.1. As situações mais comuns de furto de identidade pela internet

As principais realidades tratadas neste manual, escolhidas por serem as mais comuns, serão o *phishing* para obtenção de acesso quer à conta de *e-mail* de outra pessoa (ver o caso 5 e 9), quer à conta bancária (ver caso 4) e a difamação em redes sociais (ver casos 6 e 10).

Atentemos, de início, no *phishing* para obtenção de acesso à conta de *e-mail*. Uma vez obtidos os dados pessoais e confidenciais da vítima, através de qualquer um dos métodos mais sofisticados mencionados no capítulo anterior, o criminoso informático poderá obter acesso à conta de *e-mail* da vítima com o objectivo de tomar conhecimento do conteúdo da caixa de correio, de estabelecer contacto com o banco da vítima - normalmente com o gestor de conta - ou de utilizar aquela conta de *e-mail* para credibilizar as mensagens de correio electrónico que pretende enviar e que serão, normalmente, pedidos de ajuda financeira e formas de obter os dados pessoais de outras potenciais vítimas.

Assim, os dois objectivos principais do *phishing* para acesso à conta de *e-mail* são obter dados pessoais e confidenciais da vítima (através da consulta da sua caixa de correio electrónico ou do contacto com o Banco) para cometer burla bancária ou simplesmente ludibriar os amigos ou conhecidos das vítimas de furto de identidade, de modo a que estes procedam a transferências de montantes monetários a favor do criminoso ou que lhe forneçam os seus próprios dados pessoais. Observamos, portanto, que o *phishing* para obtenção de acesso à conta de *e-mail* da vítima pode ter, muitas vezes, como objectivo último, o acesso à respectiva conta bancária e a decorrente burla bancária.

O *phishing* “típico”, para acesso directo à conta bancária da vítima, já descrito em cima, é já, infelizmente, muito comum no nosso país.

Numa vertente diferente, surge-nos o furto de identidade para difamação em redes sociais. Este tipo de situação ocorre com frequência no âmbito das relações de amizade ou namoro, particularmente entre adolescentes e jovens.

Existem duas possibilidades de furto de identidade visando a difamação numa rede social: a criação de um perfil ou página falsos, com os dados da vítima e em seu nome, com o intuito

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

de, através de fotografias ou frases, ofender a sua honra e consideração pessoal (cfr. caso 6) e a utilização do perfil verdadeiro da vítima para difundir factos, juízos e imagens igualmente ofensivos (ver caso 10).

Nestes casos, é, normalmente, a própria vítima que, no âmbito da relação de proximidade, fornece os dados ao criminoso que permitem o seu acesso à página pessoal da vítima numa rede social ou aos factos e imagens que depois utilizará para a humilhar.

3.2. O autor do crime e a vítima

Há que distinguir, neste âmbito, entre o perfil do criminoso que comete furto de identidade com motivações lucrativas e o que pratica furto de identidade para difamação em redes sociais.

Procurando traçar o perfil do autor do furto de identidade no primeiro tipo de casos, vale a pena distinguir entre o autor que conhece a vítima porque é seu amigo, familiar ou porque mantém com ela uma qualquer relação legítima (trabalha na sua casa, é seu contabilista, advogado, *etc.*) e que, por isso, tem maior facilidade de acesso à sua informação pessoal e que a escolhe por esse motivo, e o autor desconhecido que procura vítimas aleatoriamente. Nestes casos, a identificação do perpetrador poderá revelar-se muito difícil, uma vez que, para além de muitas vezes praticar os actos criminosos a partir do “outro lado do mundo”, utiliza sempre a identidade da vítima, pelo que os seus próprios dados pessoais não são divulgados. Por este motivo, não se conhecem muitos autores destes crimes ou as suas características.

De início, via-se o cibercriminoso como um homem, estudante, especialista em informática, com Q.I. acima da média, introvertido e com limitadas capacidades de interacção social, movido pelo desafio de superação da máquina e pelo anseio de demonstrar a sua superioridade intelectual face à sociedade.

Porém, a realidade evoluiu. Hoje o autor do furto de identidade pela Internet pode ser qualquer um e a sua motivação é a de obter a informação necessária das vítimas para, com isso, granjear lucros e benefícios.

Tendo em conta a multiplicidade e variedade de meios disponíveis para a obtenção dos dados de possíveis vítimas, que podem exigir conhecimentos especializados ou implicar simplesmen-

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

te vasculhar num caixote do lixo, o perpetrador do furto de identidade pode ser uma pessoa com vasta formação ou com muito pouca, de qualquer estrato social e com as mais diversas características pessoais.

O facto de existirem várias páginas na *web* que ensinam a praticar crimes informáticos torna cada vez mais acessível ao homem comum e necessitado de dinheiro proceder a um esquema como aqueles de que temos vindo a falar.

Um tipo de autor que merece destaque neste âmbito é o chamado *insider*. Trata-se de um funcionário altamente qualificado, da confiança da entidade patronal, que aproveita os seus conhecimentos sobre a empresa e sobre o funcionamento do sistema informático e as suas falhas para obter, vender ou utilizar informação privilegiada para a prática de crimes.

Os instigadores mais perigosos deste tipo de crimes são as organizações criminosas, que controlam todo o processo do furto de identidade, desde a obtenção dos dados até ao branqueamento do capital¹⁰.

Quanto à vítima, alerte-se para o facto de poder, também, ser qualquer pessoa. O factor mais decisivo na escolha da vítima pelo criminoso será a facilidade com que este consegue obter os seus dados pessoais necessários para o crime que pretende praticar. Isto não significa que o autor do crime seja, necessariamente, alguém próximo da vítima e com acesso ao seu correio, documentos ou computador, como um familiar, amigo ou outra pessoa com uma relação legítima com a vítima, embora o possa ser muitas vezes.

Ainda assim, no Reino Unido, as estatísticas apontam para que o alvo mais comum destes criminosos sejam homens empregados entre os 40 e os 50 anos de idade¹¹. Os criminosos procuram, assim, vítimas em boa situação financeira, seja porque querem apropriar-se ilicitamente do seu património, seja porque querem atribuir credibilidade aos actos que praticam, nomeadamente tentativas de obtenção de crédito, fazendo-o em nome daquelas.

Nos Estados Unidos da América, há uma maior incidência do furto de identidade em agregados familiares com rendimentos superiores a 75.000 dólares anuais e nas camadas da população com idades entre os 16 e os 34 anos¹².

Muitas vezes as vítimas são empresas, instituições bancárias, seguradoras ou entidades finan-

10 Neste âmbito, podemos distinguir três tipos de operadores: os que obtêm a informação pessoal necessária da vítima, os que arranjam formas de usar a identidade furtada, falsificando documentos, por exemplo, e aqueles que utilizam a identidade alheia para cometer crimes. A divisão do trabalho nestas organizações criminosas visa separar os perpetradores e manter as várias partes da organização no anonimato, de modo a proteger o "todo" da organização, no caso de uma delas ser descoberta pelas autoridades policiais.

11 Sandra Peaston, *The anonymous attacker and the not so anonymous victim*, *The Anonymous Attacker*, CIFAS, 2009, p.20.

12 Cfr. Lynn Langton and Michael Planty, *Victims of Identity Theft*, 2008, Bureau of Justice Statistics Special Report, 2010, p. 3.

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

ceiras que preferem não denunciar a situação e resolver o problema ao nível interno, assumindo as perdas, por receio que o conhecimento público do ocorrido leve ao seu descrédito.

No âmbito das redes sociais, o furto de identidade é geralmente levado a cabo por pessoas com ligações de proximidade com a vítima que, por qualquer motivo, decidem prejudicá-la, por exemplo criando um perfil falso com a sua identidade ou utilizando o seu perfil verdadeiro para a difamar. Isto acontecerá, frequentemente, no âmbito de relações entre ex-namorados com desejos de vingança.

3.3. Factores de risco

Uma vez que qualquer pessoa pode ser vítima, é muito importante conhecer as circunstâncias que podem aumentar a vulnerabilidade dos utilizadores e o risco de vitimação.

As informações pessoais do indivíduo comum encontram-se cada vez mais acessíveis publicamente, nomeadamente através das redes sociais, e os criminosos informáticos tiram partido desse facto.

Há algumas condutas que aumentam o risco aquando da utilização das redes sociais, a saber:

- › Não activar as opções relacionadas com a privacidade ou manter um perfil muito acessível;
- › Disponibilizar e partilhar muita informação;
- › Aceitar pedidos de amizade de pessoas desconhecidas;
- › Publicar fotos íntimas nas redes sociais.

Trabalhar várias horas *online* aumenta o risco de se ser alvo de cibercrime, principalmente se se trabalha a partir de casa e fazendo uso do computador pessoal, visto que, ao contrário dos funcionários das empresas, que empregam técnicos informáticos que se encarregam de proteger os computadores, os trabalhadores *freelancers* possuirão computadores em regra menos protegidos para impedir ataques informáticos.

Há inúmeros comportamentos que aumentam o risco de se ser vítima de cibercrime, a saber:

- › Não ter instalado no computador um programa antivírus ou *anti-spyware*;
- › Aceder a (clicar em) *links* desconhecidos;

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

- › Assistir a conteúdos para adultos;
- › Responder a mensagens em redes sociais, a *e-mails* ou a contactos por qualquer outro meio provenientes de desconhecidos;
- › Transportar na carteira palavras-passe ou códigos PIN, ou guardar estes dados num ficheiro desprotegido;
- › Revelar, ainda que a pessoas de confiança, palavras-passe ou códigos PIN;
- › Utilizar informações de fácil acesso na criação de palavras-passe, como a data de nascimento, o nome da mãe ou do animal de estimação;
- › Guardar os documentos importantes em lugares não seguros;
- › Deitar fora documentos sem os destruir;
- › Enviar informação confidencial por *e-mail*;
- › Não proceder às actualizações dos programas antivírus e outros instalados no computador;
- › Usar ligações *wi-fi* grátis.

3.4. Impacto do furto de identidade

3.4.1. Na vítima

Apesar de a vítima poder ser qualquer pessoa, certos grupos da população, designadamente pessoas em situação financeira mais precária, minorias e pessoas idosas, sofrerão em regra um impacto emocional, físico e/ou financeiro maior, ou porque têm poucos recursos económicos, ou porque podem enfrentar obstáculos linguísticos, ou ter receio de represálias se denunciarem o crime ou não recuperar das perdas se não tiverem acesso a crédito. Para além disso, podem ter mais dificuldades em apresentar queixa, preencher formulários, ler documentos e contactar com serviços de apoio à vítima.

a. FINANCEIRO

O impacto económico pode ser de dois tipos: a perda económica directa, que se refere ao montante de dinheiro que o perpetrador obteve por usar a identidade da vítima, incluindo o valor monetário e/ou dos bens e serviços obtido, e a perda económica indirecta, que inclui todos os gastos suportados pela vítima por causa do furto de identidade (custos com os processos judiciais, chamadas telefónicas, gastos com o correio, etc). Cerca de

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

62% das vítimas de furto de identidade afirmam ter sofrido uma destas perdas económicas, de acordo com um estudo referente aos anos de 2006 e 2007¹³.

O custo financeiro total para as vítimas de furto de identidade foi próximo de 17,3 mil milhões de dólares durante o período de 2006 e 2007¹⁴ nos EUA e 388 mil milhões de dólares num total de 24 países do Mundo, durante o ano de 2011¹⁵.

Nos casos de furto de identidade para burla bancária ou relacionada com cartão de crédito, os bancos tendem a reembolsar voluntariamente as vítimas, uma vez que os valores não são significativos ao nível das instituições e que a publicidade da burla pode afectar a reputação do banco e o seu número de clientes. Porém, as instituições podem mesmo ver-se obrigadas judicialmente a indemnizar a vítima pela sua perda.

Em Portugal, a jurisprudência dos tribunais superiores tem vindo a decidir uniformemente no sentido da aplicabilidade do art.º 796º, nº 1 do Código Civil – responsabilidade pelo risco no âmbito contratual -, correndo os riscos da falha do sistema informático e de ciberataques ao mesmo por conta dos bancos quando não se prove que houve culpa da vítima, e do DL nº 317/2009, que exige também a demonstração de culpa da vítima para afastar a responsabilidade do banco. Assim, para não ter que indemnizar a vítima pelos danos sofridos, terá que ser a instituição bancária a fazer prova de que houve culpa desta.

Em casos extremos, a vítima poderá perder a sua habitação e ver as suas poupanças dizimadas. A vítima que seja alvo de uma burla para utilização da sua conta a crédito pode ter dificuldade em obter novos créditos ou empréstimos e em constituir hipotecas.

b. LEGAL

A vítima pode ser constituída arguida e acusada de crimes que não cometeu (ver caso 7).

Pode ser ré num processo por responsabilidade civil por factos que lhe são alheios ou por obrigações que não assumiu.

13 Cf. LYNN LANGTON AND MICHAEL PLANTY, *Victims of Identity Theft*, 2008, Bureau of Justice Statistics Special Report, 2010, p. 4.

14 Cf. LYNN LANGTON AND MICHAEL PLANTY, *Victims of Identity Theft*, 2008, Bureau of Justice Statistics Special Report, 2010, p. 4.

15 Norton Cybercrime Report, 2011

3. FURTO DE IDENTIDADE – A REALIDADE PRÁTICA

c. EMOCIONAL

Embora os efeitos ao nível psicológico variem de pessoa para pessoa de acordo com diversos factores, entre os quais as características da vítima, alguns sintomas mais comuns são medo, ansiedade, raiva ou mesmo uma desconfiança constante e prolongada no tempo em relação a tudo e todos, que muitas vítimas descrevem como “paranóia”. O impacto emocional do furto de identidade é descrito como sendo semelhante às reacções das vítimas de crimes violentos. Muitas sentem a sua privacidade violada, sentem-se desamparadas, impotentes e receosas de que o crime se repita.

As vítimas podem apresentar relutância em denunciar o crime de que foram vítimas às autoridades policiais caso descubram que o autor do crime é alguém próximo e em quem confiavam, como um familiar ou um amigo. Podem também sentir-se envergonhadas por terem sido ludibriadas.

A insegurança gerada pela perda de estabilidade financeira tem um impacto muito forte nestas vítimas. Acresce por vezes a necessidade de provarem a sua inocência.

Muitas vítimas culpam-se pelo que aconteceu, questionam-se em quem podem confiar e se irá fazer-se justiça.

As vítimas de furto de identidade pela Internet e do cibercrime em geral podem sentir que são tratadas como vítimas de “segunda categoria”, menos merecedoras de apoio que as restantes vítimas, uma vez que estes crimes ainda são subvalorizados socialmente e há poucos serviços que as auxiliem a recompor a sua vida. Estas vítimas têm também que saber lidar com a desilusão de, em muitos casos, não ser possível identificar o “ladrão” de identidade.

Acresce que, conforme vai tomando conhecimento de novas dívidas ou outras consequências do crime, a vítima vai sendo alvo de constante revitimação.

Os efeitos do crime diferem quando o seu autor é alguém próximo da vítima. Nestes casos, as vítimas podem sentir-se pressionadas a assumir responsabilidade pelo sucedido, para proteger o criminoso das respetivas consequências.

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

d. IMPACTO NA ROTINA DIÁRIA

O furto de identidade implica, para a vítima, um sério aborrecimento e muito tempo perdido para reparar as suas consequências. Nos EUA, estima-se que as vítimas gastem, em média, 97 horas na reparação dos danos causados pelo crime, despendendo com esta actividade, também em média, 1.884 dólares (dados da organização americana Identity Theft Resource Center). Já no Reino Unido, a vítima gastará entre 3 e 48 horas a “limpar o seu nome”¹⁶.

40% das vítimas afirma que a perda de tempo foi a pior consequência do crime¹⁷.

3.4.2. Na sociedade

No Reino Unido, o custo do furto de identidade para a economia do país foi calculado em 1,3 mil milhões de libras por ano. Na Austrália, as perdas anuais variam entre mil milhões de dólares e mais de 3 mil milhões. Nos Estados Unidos, no ano de 2005, estima-se que as perdas tenham sido de 56,5 mil milhões de dólares¹⁸. No distrito de Lisboa, os danos do *phishing* no ano de 2011 foram superiores a 2 milhões de euros¹⁹.

O furto de identidade tem um custo crescente para instituições como bancos, companhias de seguros e empresas fornecedoras de bens e serviços. Estas instituições podem ter que suportar a perda económica de que a vítima é alvo, a não ser que se prove que esta foi negligente. Este impacto para as instituições não deve ser de descurar, mais que não seja porque acabará por se reflectir nos custos que o consumidor terá que suportar para usufruir dos serviços da empresa.

As próprias empresas podem ver as suas identidades ilicitamente utilizadas e, nesses casos, bem como naqueles em que são usados dados dos seus clientes, as perdas indirectas relacionar-se-ão com investigações entre os funcionários, a aposta na prevenção e a contratação de seguros.

O descrédito que pode afetar estas empresas também não deve ser subestimado, pelo seu impacto no sistema económico.

Os Estados e os seus governos podem sofrer perdas directas, uma vez que muitos furtos de identidade são cometidos em relação a organismos públicos, mas sofrem, sobretudo, perdas indirectas, uma vez que têm que concentrar fundos na prevenção, na formação de profissionais, designadamente das autoridades judiciais e policiais e na dotação destas com meios de investigação e combate a estes fenómenos criminais.

16 Fraud prevention expert group, Report on identity theft/fraud, Bruxelles, 2007, p. 10.

17 Norton Cybercrime Report, 2011.

18 Marco Gercke, Internet-related identity theft, Economic Crime Division, Directorate general of Human and Legal Affairs, Strasbourg, France, Council of Europe, 2007, pp 5 e 6.

19 <http://www.asjp.pt/2012/04/03/judiciaria-cria-unidade-especial-para-investigar-cibercrime/>

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

3.5. Dificuldades na investigação

O furto de identidade através da Internet, e o cibercrime em geral, levantam sérios problemas para as autoridades policiais e judiciárias no que à investigação diz respeito. As próprias características do crime, assim como outros factores com ele relacionados, tornam a identificação dos autores das condutas e a definição das circunstâncias do crime muito difíceis ou mesmo, por vezes, quase impossíveis.

O furto de identidade tem uma dimensão internacional, transfronteiriça, tal como o cibercrime em geral. Se o perpetrador e a vítima não se encontram no mesmo país a investigação é dificultada, uma vez que, para além de se ter que seguir um rasto cibernético que cobre potencialmente o Mundo, requer a cooperação das autoridades policiais e judiciárias de todos os países envolvidos. O princípio da soberania não permite que um país leve a cabo investigações noutro país sem a permissão das autoridades locais. A cooperação entre as autoridades dos países acarreta formalidades e tempo, o que prejudica as investigações.

Diz-se que o cibercrime é atemporal uma vez que entre a prática da acção inicial pelo autor e a sua materialização final na produção de um resultado pode existir uma separação temporal indefinida, o que não facilita igualmente a investigação.

Muitos dos processos que o cibercrime envolve podem ser automatizados (atente-se no *spamming*) para se repetirem, dotando o crime de permanência.

Os criminosos usam tecnologias que lhes permitem permanecer no anonimato, como o *spoofing* e outros programas de anonimização e codificação.

O elevado grau de tecnicidade que a investigação do cibercrime requer implica o envolvimento de várias entidades com conhecimentos específicos e ainda a utilização de muitos recursos internos, logísticos e humanos, que são limitados.

Acrescem a estas especificidades outros fatores que prejudicam a investigação.

Estima-se que 80% das vítimas de cibercrime não denuncie o crime às autoridades.²⁰ Este facto deriva da falta de consciência da sua condição de vítima e de informação sobre os meios de denunciar, assim como da crença na ineficácia da investigação criminal nestes casos e na

20 United Nations
Office on Drugs and Crime,
Comprehensive Study on Cy-
bercrime - Draft, February
2013, p. 117.

3. FURTO DE IDENTIDADE - A REALIDADE PRÁTICA

impunidade destes crimes. Outro motivo para as vítimas não fazerem queixa é a vergonha que sentem por terem sido enganadas.

Como já acima se referiu, as empresas, bancos, seguradoras e entidades financeiras optam por lidar com o problema internamente, absorvendo as perdas, e por não apresentar queixa às autoridades, por receio de que o conhecimento público do ataque informático leve ao seu descrédito e à perda de confiança por parte do mercado e dos clientes.

O número de vítimas aumenta a cada dia, conforme aumenta o número de utilizadores da Internet.

Existem páginas disponíveis *online* que contêm informações sobre como cometer certos crimes informáticos e é simples chegar até elas através de pesquisas nos motores de busca mais conhecidos.

A cada dia também, os criminosos criam novas formas de aceder a dados pessoais e de praticar crimes com base na utilização destes. As novas técnicas difundem-se rapidamente através do mercado negro *online*.

Um grande obstáculo à investigação do cibercrime é a séria dificuldade que existe em aceder à prova electrónica. Para localizar a origem da comunicação, ou seja, o endereço IP (ou *Internet Protocol Address*), é necessário o acesso ao registo dos ficheiros históricos arquivados pelos fornecedores de serviços de Internet, cuja colaboração é essencial.

É também muito importante assegurar a validade da prova digital. Assim, o acesso, recolha, conservação e análise devem ser sempre efectuados de acordo com procedimentos específicos, competindo essa tarefa a especialistas. A recolha da prova tem que ser feita o mais rapidamente possível, uma vez que esta é muito facilmente destruída. Para que isto seja viável, é fundamental a cooperação dos fornecedores de serviços de Internet, sendo que estes só são obrigados a preservar certos dados e durante um período de tempo limitado.

4.

QUADRO LEGAL

[illegible]

4. QUADRO LEGAL

A implementação de legislação adequada desempenha um papel essencial na prevenção e combate ao cibercrime.

A sua existência é importante no âmbito da criminalização das condutas, das competências e poderes de investigação das autoridades policiais, da recolha e preservação de prova electrónica, da jurisdição, da cooperação e partilha de informações, tanto entre diferentes entidades nacionais como ao nível internacional, e da responsabilidade dos fornecedores de serviços de Internet.

Embora ao nível nacional os Estados se foquem mais na criminalização das condutas, tem-se vindo a reconhecer a necessidade de desenvolver legislação respeitante às outras matérias.

4.1. Enquadramento internacional

Os últimos anos têm revelado uma grande preocupação internacional no combate ao cibercrime. Destaca-se a actividade desenvolvida nesta área pelo Conselho da Europa, União Europeia e Organização das Nações Unidas.

A Convenção sobre o Cibercrime do Conselho da Europa (CCCE) de 23 de Novembro de 2001 é o instrumento internacional mais utilizado para o desenvolvimento de legislações nacionais sobre cibercrime.

A CCCE, perante a informatização do Mundo e o risco de que as novas tecnologias e a Internet sejam utilizadas para praticar crimes, visa prosseguir uma política criminal comum que proteja a sociedade do cibercrime, através da adopção de legislação harmonizada e da cooperação internacional. Debruçar-nos-emos *infra* sobre os crimes que este instrumento internacional estabelece e sobre a sua aplicação às diferentes fases do furto de identidade através da Internet, conforme o definimos.

No âmbito da União Europeia destacam-se a Decisão-Quadro 2005/222/JAI sobre ataques a sistemas de informação e a Directiva 2013/40/EU do Parlamento Europeu e do Conselho, que veio substituir aquela.

A Decisão-Quadro 2005/222/JAI visava melhorar a cooperação entre as autoridades judiciais e policiais dos Estados-Membros e harmonizar as normas penais sobre o cibercrime.

4. QUADRO LEGAL

A Directiva 2013/40/EU do Parlamento Europeu e do Conselho veio, como já se referiu, substituir a Decisão-Quadro e estabelece como seu principal objectivo «*aproximar as legislações dos Estados-Membros na área dos ataques contra sistemas de informação, estabelecendo regras mínimas sobre a definição dos tipos legais de crime, e melhorar a cooperação entre as autoridades competentes (...)*». Estabelece os crimes de acesso ilegal, interferência ilegal em sistema informático, interferência ilegal de dados e interceptação ilegal. O art.º 7º prevê o crime de uso de instrumentos para cometer infracções e aplica-se à segunda fase do furto de identidade.

4.2. Lei portuguesa

No que à lei nacional diz respeito, o quadro de referência resulta, em primeiro lugar, da Lei nº 109/2009 de 15 de Setembro, a Lei do Cibercrime (LC), que transpõe para o nosso ordenamento a Decisão-Quadro 2005/222/JAI e adapta o direito interno à CCCE. Nas seguintes tabelas analisam-se os tipos legais de crime previstos nos arts.º 3º a 8º desta lei:

Artigo e epígrafe	Condutas	Artigo correspondente da CCCE
Art. 3º - Falsidade informática	Introdução, modificação, eliminação ou supressão de dados informáticos com intenção de provocar engano nas relações jurídicas ou interferência, por qualquer outro modo, num tratamento informático de dados, produzindo dados ou documentos falsos, com intenção de que estes sejam considerados ou utilizados para finalidades jurídicas relevantes como se fossem verdadeiros.	Art. 7º
Art. 4º - Dano relativo a programas ou outros dados informáticos	Apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, sem permissão legal ou sem estar autorizado	Art. 4º

4. QUADRO LEGAL

|||||

4. QUADRO LEGAL

Artigo e epígrafe	Condutas	Artigo corres-pondente da CCCE
Art. 3º, nº 4 - Falsidade informática	Importar, distribuir, vender ou deter para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado sobre os quais tenham sido praticadas as acções vedadas pelo nº 2 do artigo - introduzir, modificar, apagar ou suprimir dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, produzindo dados ou documentos falsos, com intenção de que estes sejam considerados ou utilizados para finalidades jurídicas relevantes como se fossem verdadeiros.	Art. 6º, nº 1, als. a) e b)
Art. 4º, nº 3 - Dano relativo a programas ou outros dados informáticos	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas pelo nº 1 do artigo.	
Art. 5º, nº 2 - Sabotagem informática	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas pelo nº1 do artigo.	
Art. 6º, nº 2 - Acesso ilegítimo	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas	



4. QUADRO LEGAL



	informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas pelo nº 1 do artigo.
Art. 7º, nº 3 - Intercepção ilegítima	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizada pelo nº 1 do artigo.

Os arts.º 11º a 19º estabelecem normas relativamente ao direito processual, que permitem a recolha expedita e manutenção da prova electrónica, no seguimento do que é estabelecido pela CCCE nos arts.º 14º a 21º.

O art.º 11º começa por estabelecer o âmbito de aplicação das disposições processuais. Assim, os arts.º 11º a 19º aplicam-se aos crimes previstos nesta lei, àqueles que sejam cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

O artº. 12º estabelece que, se no decurso do processo, e tendo em vista a descoberta da verdade, for necessário em termos de produção de prova obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa. A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente, ou mesmo sem esta quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva-os de imediato, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigada a assegurar a confidencialidade da aplicação da medida processual.



4. QUADRO LEGAL

O art.º 13º, que tem como escopo assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, estabelece que o fornecedor de serviço a quem, nos termos do artigo 12º, essa preservação tenha sido ordenada deve indicar à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

O art.º 14º prevê a injunção para apresentação ou concessão do acesso a dados. Assim, se no decurso do processo se tornar necessário à produção de prova obter dados informáticos específicos e determinados armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. Este mecanismo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços. Esta injunção não pode ser dirigida a suspeito ou arguido no processo. Não pode igualmente fazer-se uso desta injunção quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista. O regime de segredo profissional ou de funcionário e de segredo de Estado é aqui aplicável.

O art.º 15º consagra a pesquisa de dados informáticos, permitindo que se se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados armazenados num determinado sistema informático no decorrer do processo, a autoridade judiciária competente autorize ou ordene por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

O art.º 16º refere que, se no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena, por despacho, a apreensão dos mesmos. O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15º, bem como quando haja urgência ou perigo na demora.

4. QUADRO LEGAL

O art.º 17º estabelece de forma similar que, se no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

O art.º 18º consagra o regime da interceptação e registo de transmissões de dados informáticos, que só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

Finalmente, o art.º 19º estabelece a possibilidade de recurso a acções encobertas.

Os arts.º 20º a 26º relacionam-se com a cooperação internacional e o art.º 27º com a jurisdição territorial, também no rasto do que preveem os arts.º 23º a 35º e 38º da CCCE, respetivamente.

Quanto à lei portuguesa, atente-se ainda em algumas das normas do Código Penal (CP) que, maioritariamente, terão aplicabilidade a casos de furto de identidade pela Internet: a devassa da vida privada, prevista no art.º 192º, a devassa por meio de informática, consagrada no art.º 193º, a violação de correspondência ou telecomunicações, criminalizada pelo art.º 194º, o furto, tipificado no art.º 203º, a gravação e fotografias ilícitas, previstas pelo art.º 199º e a burla informática, estabelecida pelo art.º 221º deste diploma. Atente-se na seguinte tabela:

CÓDIGO PENAL PORTUGÊS		
Artigo e epígrafe	Condutas	Tipo de crime
Art. 192º - Devassa da vida privada	Interceptar, gravar, registar, utilizar, transmitir ou divulgar uma conversa, uma comunicação telefónica, mensagens de correio electrónico ou facturação detalhada; captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos; observar ou escutar às ocultas pessoas que se	Semi-público

4. QUADRO LEGAL

	encontrem em lugar privado ou divulgar factos relativos à vida privada ou a doença grave da vítima, sem consentimento da vítima e com intenção de devassar a vida privada desta, nomeadamente a sua intimidade familiar ou sexual.	
Art. 193º - Devassa por meio de informática	Criar, manter ou utilizar ficheiro de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou à origem étnica.	Público
Art. 194º - Violação de correspondência ou telecomunicações	Abrir uma encomenda, uma carta ou qualquer outro escrito que se encontre fechado e que não lhe seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário; intromissão no conteúdo das telecomunicações ou tomar conhecimento das mesmas e divulgar o conteúdo de escritos fechados ou telecomunicações.	Semi-público
Art. 199º - Gravação e fotografias ilícitas	Sem consentimento, gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; utilizar ou permitir que se utilizem as gravações referidas, mesmo que lícitamente produzidas; fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado ou utilizar ou permitir que se utilizem fotografias ou filmes já referidos, mesmo que lícitamente obtidos.	Semi-público
Art. 203º - Furto	Subtrair um objeto com intenção de apropriação.	Semi-público
Art. 221º - Burla informática	Interferir no resultado de tratamento de dados ou estruturar incorrectamente programa informático, utilizar incompleta ou incorrectamente dados, a utilizar dados ou intervir por qualquer modo no processamento, sem autorização, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial.	Semi-público

4. QUADRO LEGAL

4.3. O furto de identidade, a lei nacional e a Convenção do Cibercrime

À primeira fase, de obtenção dos dados relativos à identidade de alguém e que permite o furto de identidade, serão aplicáveis o art.º 3º da LC – falsidade informática- e o correspondente art. 7º da CCCE, o art.º 6º da LC - acesso ilegítimo – e o correspondente art.º 2º da CCCE, o art.º 7º da LC – interceptação ilegítima - e o similar art.º 3º da CCCE e os arts.º 4º e 5º da CCCE, respetivamente relativos à interferência com dados e com sistemas.

Serão igualmente aplicáveis tipos legais previstos no CP. A devassa da vida privada tem aplicabilidade nesta primeira fase, uma vez que criminaliza as condutas de interceptar, gravar, registar uma conversa, uma comunicação telefónica, mensagens de correio electrónico ou facturação detalhada, de captar, fotografar, filmar, registar imagens das pessoas ou de objectos ou espaços íntimos ou observar ou escutar às ocultas pessoas que se encontrem em lugar privado, condutas estas que podem permitir a obtenção dos dados pessoais de uma vítima. O mesmo se pode dizer em relação à violação de correspondência ou de telecomunicações, tendo em conta que abrir uma encomenda, uma carta ou qualquer outro escrito que se encontre fechado e que não seja dirigido ao autor, tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, assim como a intromissão no conteúdo das telecomunicações ou a tomada de conhecimento das mesmas são, igualmente, formas de conhecer os dados pessoais da vítima e outra informação privada. O crime de gravações e fotografias deve também ser mencionado na análise da criminalização da primeira fase do furto de identidade, visto que gravar palavras proferidas por outra pessoa e não destinadas ao público ou fotografar ou filmar outra pessoa permite também a pesquisa e obtenção de dados sobre as vítimas. O furto de documentos e afins permite igualmente a obtenção de informação relevante para o furto de identidade. A burla informática parece também poder inserir-se neste âmbito, uma vez que as condutas de obtenção de informação com objectivo lucrativo cabem no cerne de comportamentos que este crime pretende punir.

À fase da posse ou transferência aplicam-se os arts.º 3º, nº4, art.ºº 4, nº3, art.º 5º, nº 2, art.º 6º, nº 2, art.º 7º, nº 3 da LC e o art.º 6º da CCCE.

Parecem ter aplicação a esta fase também a devassa da vida privada, por punir a transmissão de mensagens de correio electrónico ou facturação detalhada e a devassa da privacidade por meio de informática, por criminalizar a manutenção de um ficheiro de dados individualmente identificáveis.

4. QUADRO LEGAL

À terceira fase, da utilização da identidade alheia para a prática de crimes, poderá aplicar-se qualquer tipo legal correspondente ao crime praticado fazendo uso dessa identidade. Por referência ao caso 7, diga-se que Joana que, utilizando os dados identificativos de Juliana, praticou o crime de burla informática, incriminando-a por este, deveria ser punida exactamente por tal crime (art.º 221º do CP).

Dos crimes que mencionámos, diga-se que a devassa da vida privada terá aplicação nesta terceira fase, visto punir a divulgação de uma conversa, de uma comunicação telefónica, de mensagens de correio electrónico ou de facturação detalhada, a divulgação da imagem de pessoas, objectos ou espaços íntimos e a divulgação de factos relativos à vida privada ou a doença grave da vítima. A devassa da privacidade por meio de informática será também aplicável, uma vez que criminaliza a utilização de ficheiros de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada ou à origem étnica. As gravações e fotografias ilícitas fazem parte do núcleo de tipos legais que punem as condutas incluídas nesta terceira fase, visto sancionarem a utilização ou permissão de utilização das gravações de palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas, e das fotografias ou filmes de outra pessoa, mesmo em eventos em que tenha legitimamente participado.

A burla informática – art.º 221º do CP e art.º 8º da CCCE- e o acesso ilegal –art.º 6º da LC e art.º 2º da CCCE - são, muitas vezes, os crimes aplicáveis a esta fase da utilização dos dados identificativos de alguém, nomeadamente nos casos de *phishing*.

5.

APLICAÇÃO DA LEI NACIONAL AOS CASOS TÍPICOS

[illegible]

5. APLICAÇÃO DA LEI NACIONAL AOS CASOS TÍPICOS²¹

< Caso 1 >

A Josué aplica-se o crime de acesso ilegítimo (art.º 6º, nº2 da LC) e à organização criminosa o mesmo crime (art.º 6º, nº 1 da LC) e o crime de burla informática (art.º 221º, nº 1 do CP).

< Caso 2 >

Ao caso de Joana aplica-se, no que respeita à utilização da técnica de *keylogging* para obter os dados de acesso à sua conta bancária, o tipo legal de interceptação ilegítima (art.º 7º, nº 1 da LC). Já com referência à utilização dos dados obtidos para entrar na conta *online* e retirar de lá o dinheiro, aplica-se o crime de acesso ilegítimo (art. 6º, nº 1 da LC) e de burla informática (art.º 221º, nº 1 do CP).

< Caso 3 >

O caso 3 não constitui uma situação de furto de identidade, a não ser que o criminoso tenha obtido dados de Jandira. Aplica-se a esta situação, tal como se encontra descrita, o crime de acesso ilegítimo (art.º 6º, nº 1 da LC), de dano informático (art.º 4º, nº 1 da LC), de sabotagem informática (art. 5º, nº 1 da LC) e o crime de extorsão (art.º 223º, nº 1 do CP).

< Caso 4 >

Neste caso típico de *phishing* aplica-se o crime de falsificação de documentos (art.º 256º, nº 1, al. a) do CP) à criação de um e-mail falso, o tipo legal de falsidade informática (art. 3º, nº 1 da LC) à criação de uma página da *web* falsa, o crime de acesso ilegítimo (art.º 6º, nº 1 da LC) ao acesso à conta online de Josefina e a burla informática (art.º 221º, nº 1 do CP) à transferência do dinheiro da sua conta para outra.

21 A análise que se segue pretende somente referir quais as normas legais que têm aplicação aos casos descritos, para que se entenda a relação entre os crimes e os seus elementos e o tipo de condutas em estudo. A questão do concurso que eventualmente existirá, em certos casos, entre as normas legais que têm aplicabilidade ao caso, assim como a forma de resolução desse concurso, não será abordada.

5. APLICAÇÃO DA LEI NACIONAL AOS CASOS TÍPICOS

< Caso 5 >

O *spamming* é punido pelo crime de sabotagem informática (art.º 5º, nº 1 da LC). Aplica-se o crime de falsificação de documentos (art.º 256º, nº 1, al. a) do CP) à criação de um e-mail falso e o crime de acesso ilegítimo (art.º 6º, nº 1 da LC) ao acesso à conta de e-mail.

Parece existir igualmente burla informática (art. 221º, nº 1 do CP) na sua forma tentada.

< Caso 6 >

Jéssica terá que fazer queixa do comportamento de Joel e deduzir acusação particular, uma vez que a conduta deste preencherá o crime de difamação (art.º 180º, nº 1 do CP), agravado pela publicidade, nos termos previstos pelo art.º 183º, nº 1, al. a) do CP. Joel imputou a Jéssica factos ofensivos da sua honra e consideração e difundiu estas ofensas por um meio que facilita a sua divulgação. À criação de uma página de *Facebook* falsa deverá ser aplicado o crime de falsidade informática (art.º 3º, nº 1 da LC).

< Caso 7 >

À conduta de Joana aplica-se o tipo legal de burla informática (art.º 221º, nº 1 do CP).

< Caso 8 >

Julieta foi vítima de burla informática (art.º 221º, nº 1 do CP).

5. APLICAÇÃO DA LEI NACIONAL AOS CASOS TÍPICOS

< Caso 9 >

À criação de um e-mail falso aplica-se o crime de falsificação de documentos (art.º 256º, n.º 1, al. a) do CP), ao acesso à conta de e-mail da mulher de Júlio aplica-se o crime de acesso ilegítimo (art.º 6º, n.º 1 da LC) e aplica-se igualmente o crime de burla informática (art.º 221º, n.º 1 do CP) na sua forma tentada às tentativas de obtenção de crédito em nome de Júlio.

< Caso 10 >

Jaime, na posse dos dados necessários para obter acesso à conta de *Facebook* de Jair, acedeu a esta e publicou fotografias tiradas no âmbito da vida privada de Jair, sem o seu consentimento. Estão aqui em causa os crimes de acesso ilegítimo (art.º 6º, n.º 1 da LC), devassa da vida privada (art.º 192º, n.º 1 do CP) e de devassa por meio de informática (art.º 193º, n.º 1 do CP).

6.

PREVENÇÃO

[illegible]

6. PREVENÇÃO

De acordo com um estudo da Comissão Europeia de 2012, 70% da população estudada já tinha ouvido ou visto informação sobre o cibercrime, 31% da mesma população considera-se bastante bem informada sobre o cibercrime como risco e 7% considera-se muito bem informada²².

Outro estudo, incidindo sobre mais de 13,000 utilizadores da Internet em 24 países, demonstrou que 90% desta população apaga *e-mails* suspeitos recebidos de desconhecidos e 80% usa antivírus e não abre anexos ou *links* surgidos em *e-mails* ou mensagens de desconhecidos²³.

Porém, no que às redes sociais respeita, apenas 50% afirmou usar as opções de privacidade que aquelas oferecem para controlar a informação que partilham e com quem a partilham e 35% das pessoas aceitam pedidos de amizade de desconhecidos.

Estudos junto de crianças e adolescentes em países menos desenvolvidos demonstram que esta faixa etária apresenta riscos mais elevados de vitimação. Um estudo incidindo sobre uma população de mais de 25,000 crianças em idade escolar de 7 países na América Central e na América do Sul demonstrou que de cerca de 45% das crianças que tinham ligação à Internet em casa, apenas 10% tinham protecção antivírus ou *web filtering* no computador.

Os Estados devem investir em recursos para educar a população antes que os seus cidadãos se tornem vítimas. Instruir as comunidades para que se protejam de antemão contra o furto de identidade é a medida mais eficaz para fazer face a este fenómeno.

6.1. Medidas de prevenção

Ao usar as redes sociais, o/a utente deve:

- › Ter atenção à informação que torna pública nas redes sociais: não publicar informação que o/a torne vulnerável, mas apenas informação cujo conhecimento por qualquer pessoa não o/a possa prejudicar;
- › Ter atenção à informação que terceiros tornam pública *online* sobre si;
- › Ter atenção às pessoas a quem dá acesso à informação privada;
- › Estar atento às abordagens de pessoas que não se conhece;
- › Ser céptico e não acreditar em tudo que lhe dizem ou que lê *online*;
- › Conhecer as condições que aceita ao entrar numa rede social, as quais muitas vezes

22 European Commission. 2012. *Special Barometer* 390.

23 Symantec. 2012. *Norton Cybercrime Report* 2012.

6. PREVENÇÃO

incluem a perda de direitos sobre os conteúdos difundidos.

Ao usar o *e-mail*, o/a utente deve:

- › Ter em atenção que os *e-mails* escritos em mau português, com erros ortográficos, erros gramaticais, frases pouco coerentes ou até termos brasileiros provavelmente farão parte de esquemas de *phishing*, mesmo que tenham origem num remetente conhecido: assim acontecerá, designadamente, com *e-mails* que anunciem que venceu algum prémio, que é finalista num concurso, que existe um problema com a conta de *e-mail* ou que é necessário validar os dados bancários ou de outro sistema;
- › Não fazer o *download* de anexos, não carregar nos *links* indicados e não responder a *e-mails* de desconhecidos ou que se mostrem suspeitos pelo seu conteúdo;
- › Procurar reconhecer o endereço ao receber um *e-mail* de uma instituição bancária ou de qualquer outra com quem trabalha: se não reconhecer, contactar a instituição e procurar saber se a mensagem de correio electrónico provém realmente dela;
- › Passar o rato sobre qualquer *link* antes de carregar no mesmo, verificando no canto inferior esquerdo do *browser* para que endereço será encaminhado/a;
- › Caso o domínio do *link* seja externo ao domínio da entidade que supostamente envia o *e-mail*, o utente deve abster-se de clicar;
- › Em caso de dúvida, validar o *link* através do site <https://www.virustotal.com/pt/#url> ou através de um contacto de apoio representante da suposta entidade remetente do *e-mail* ou aceder ao site www.cert.pt e contactar com uma equipa CERT;
- › Se receber uma mensagem de *e-mail* de alguém que conhece mas que não parece corresponder ao habitual dessa pessoa, contendo um pedido de ajuda ou pedindo para fornecer dados pessoais, o utente deve desconfiar, uma vez que a conta de *e-mail* poderá ter sido comprometida por um cibercriminoso;
- › Evitar a utilização da conta de *e-mail* profissional para uso pessoal;
- › Não utilizar o correio electrónico para enviar informação confidencial;
- › Manter o programa usado para enviar correio electrónico actualizado;
- › Desligar as opções que permitem abrir ou executar automaticamente ficheiros ou programas anexados às mensagens;
- › Desligar opções de execução de *JavaScript*, *ActiveX* ou programas *Java*.

6. PREVENÇÃO

Para proteger o computador e os dispositivos móveis, o utente deve:

- › Evitar a criação de situações propícias ao furto de computadores, telemóveis e *tablets*, deixando-os no carro, por exemplo;
- › Proteger o computador contra utilizadores mal-intencionados, atribuindo-lhe uma palavra-passe de acesso à sessão e encerrar a sessão sempre que não se esteja a utilizar o computador;
- › Ao ceder o computador, ter em atenção os dados pessoais que possa conter, tendo em conta que os dados gravados no disco rígido poderão ser acedidos, mesmo que estejam guardados numa conta protegida por palavra-passe;
- › Ao vender ou deitar ao lixo o seu computador, telemóvel ou *tablet*, apagar toda a informação pessoal que aqueles possam conter;
- › Manter sempre o computador actualizado com antivírus, *anti-spyware*, *firewall* e protecção *anti-spam*;
- › Configurar o *browser* utilizado para impedir o armazenamento de *cookies* e *pop-ups*;
- › Elevar o nível de segurança do *browser* para médio ou alto;
- › Ter sempre atenção aos programas instalados, verificando a sua proveniência – devem provir da empresa que os criou ou de um *website* fiável;
- › Evitar fazer *login* em *websites* em que partilha informação pessoal a partir de redes públicas ou abertas de *wi-fi* ou a partir de computadores que não conhece;
- › Ter atenção aos *websites* onde são fornecidos dados pessoais, sobretudo bancários – evitar *sites* com erros ortográficos ou tipográficos óbvios e sem indicações de segurança;
- › Verificar sempre se a ligação a um *website* se está a fazer através de “https” – modo seguro - e não “http” – modo não seguro – e, adicionalmente, deverá verificar se aparece um ícone representando um cadeado ou uma chave;
- › Usar apenas o *website* oficial do seu banco. Para saber qual é, escrever o nome do banco no *browser* de Internet;
- › Ler as políticas de privacidade dos *sites* das instituições financeiras ou outras em que a interacção envolva a revelação de dados pessoais e, se não as compreender ou aceitar, pondere optar por outras instituições;
- › Nos dispositivos móveis, a protecção do ecrã deverá estar activada;
- › Activar a funcionalidade de remoção remota de conteúdos se existir informação sensível armazenada no dispositivo²⁴;
- › Efectuar regularmente cópias de segurança do seu dispositivo e ter particular cuidado com elas (guardar as cópias de forma cifrada com uma boa palavra-passe).
- › Ao instalar aplicações no dispositivo, verificar se efectua o *download* de uma fonte

24 Existem aplicações/ serviços gratuitos para os diversos tipos de dispositivos que permitem em caso de perda ou roubo, apagar todos os dados de forma remota (no caso de se tratar de um Android as aplicações são a Mobile Defense ou a WaveSecure e tratando-se de um Iphone existem aplicações como a Find My Iphone ou a MobileMe).

6. PREVENÇÃO

segura e fiável e ter atenção ao tipo de permissões que estas solicitam – por exemplo, se uma aplicação que, à partida, não necessita de acesso ao *e-mail* solicitar tal acesso, deverá optar-se por uma alternativa.

Para proteger documentos de identificação e dados pessoais, o utente deve:

- › Guardar na carteira apenas os documentos necessários ao dia-a-dia;
 - › Guardar a carteira num local seguro no trabalho;
 - › Guardar os documentos em local seguro em casa, como um cofre;
 - › Destruir sempre os documentos físicos ou digitais que possam conter dados pessoais ou outras informações da mesma natureza, de modo a impossibilitar a sua consulta;
 - › Quando pedir novos cheques, solicitar que estes sejam enviados para a estação de correios e não para casa;
 - › Ter pouca informação pessoal impressa nos cheques bancários;
 - › Confirmar a legitimidade de quem pede os seus dados pessoais pelo telemóvel ou telefone, por *e-mail* ou por qualquer outro meio, e a necessidade de tal pedido:
-
- » Solicitar a identificação do interlocutor e o contacto geral da entidade que supostamente representa, averiguando se existe a possibilidade de não fornecer qualquer dado de imediato e posteriormente devolver o contacto para o efeito proposto;
 - » Procurar pensar naquilo que quem o/a contacta precisa de saber: a instituição financeira com que trabalha pode necessitar de saber o nome de solteira da sua mãe para verificar a sua identidade quando você telefona para obter informações sobre a sua conta; porém, se alguém lhe ligar ou enviar um *e-mail* a perguntar qual o nome de solteira da sua mãe, afirmando pertencer à sua instituição financeira, lembre-se que esta pessoa não necessita de obter tal informação, uma vez que esta já consta da sua ficha na instituição - o propósito de tal chamada ou mensagem de correio electrónico será pura e simplesmente obter a informação para benefício próprio;
 - » Se um desconhecido lhe telefonar ou enviar um *e-mail* a informar que ganhou um prémio ou qualquer benefício e pedir os seus dados pessoais, peça o envio de uma ficha escrita de candidatura; se não enviarem termine o contacto; se enviarem, leia-a atentamente e, quando a enviar, garanta que a endereça a uma empresa ou instituição financeira conhecida e com boa reputação.

6. PREVENÇÃO

- › Em viagem, para fornecer informações pessoais a alguém de confiança, por telefone, certificar-se de que ninguém está por perto a escutar;
- › Informar as empresas ou instituições financeiras que não devem partilhar os seus dados pessoais;
- › Armazenar as informações importantes em ficheiros e directórios protegidos por palavra-passe;
- › Encriptar os dados mais importantes.

Ao usar os correios, o utente deve:

- › Procurar manter a inviolabilidade da sua caixa de correio, usando uma boa fechadura;
- › Evitar que a correspondência se acumule ao ponto de permitir a sua remoção pelo local destinado à entrada;
- › Quando estiver em viagem, pedir junto dos correios que a sua correspondência fique na estação de correios mais próxima da sua residência ou pedir a um parente, amigo ou vizinho de confiança para recolher e guardar o correio;
- › Tentar controlar a chegada da correspondência que é previsível, nomeadamente aquela que contenha cartões de débito ou crédito, extractos bancários ou facturas;
- › Se possível, recolher e enviar as cartas que contenham a sua informação pessoal ou documentos na estação dos correios;
- › Proibir a emissão de correspondência para locais onde já não se habite e solicitar nos correios o reencaminhamento da correspondência.

Para fazer transacções financeiras em segurança, o utente deve:

- › Efectuar transacções financeiras *online* apenas através de *websites* seguros, com endereços que comecem por “https:”- adicionalmente deve verificar-se a existência de um ícone de um cadeado ou chave;
- › Verificar se está a utilizar o site oficial do seu banco;
- › Ter em atenção que os bancos nunca pedem mais do que uma pequena parte dos números (normalmente três) que constam do cartão matriz para que se possa realizar operações *online*;
- › Ter em atenção que os bancos não solicitam a instalação de aplicações no telemóvel para reforçar a segurança das suas operações – estas aplicações são normalmente vírus;
- › Em caso de dúvida contactar o banco telefonicamente;
- › Manter aplicações como o *Java* e o *Flash* atualizados;
- › Proteger todas as contas de crédito com palavra-passe.

6. PREVENÇÃO

Para conversar em Instant Messengers, IRC's e Chats online em segurança, o utente deve:

- › Usar um nome falso que não permita a sua identificação;
- › Utilizar salas com moderador (só se aplica às salas de *chat*);
- › Manter a sua informação pessoal secreta;
- › Registar as sessões de *chat*;
- › Não abrir anexos de *e-mail* que lhe sejam enviados em conversas de *chat*.

Para criar palavras-passe seguras, o utente deve:

- › Evitar sequências previsíveis;
- › Evitar, igualmente, a criação de senhas com proximidade entre caracteres do teclado. Para além de serem conhecidas, são facilmente identificáveis no momento da digitação;
- › Não usar elementos pessoais associados a si ou conhecidos por mais pessoas tais como data de nascimento, partes do nome e apelidos, morada, números de identidade ou de contribuinte;
- › Utilizar senhas com o comprimento máximo permitido e que não recorram à utilização de palavras existentes no dicionário de língua portuguesa ou qualquer outra;
- › Combinar letras, números e símbolos de modo não sequencial;
- › Ser criativo (por exemplo, pensar numa frase com um dado significado e utilizar a primeira letra de cada palavra da frase como palavra-passe);
- › Alternar entre letras maiúsculas e minúsculas e substituir letras por números ou símbolos;
- › Atribuir uma palavra-passe diferente para cada serviço (se houver necessidade de anotar, guardar a anotação física num local seguro e não num ficheiro no computador);
- › Mudar de palavras-passe regularmente.

NOTA: Os pais ou outros responsáveis por crianças e jovens deverão monitorizar as actividades daqueles *online*, garantindo que estes adoptam as mencionadas medidas de prevenção.

6.2. Sinais de infeção do computador por *malware*

O facto de o computador do utente estar infectado por vírus indica uma maior probabilidade de aquele poder ser vítima de furto de identidade. Assim, importa conhecer os sintomas da infecção de um computador por vírus:

6. PREVENÇÃO

- › Lentidão;
- › Bloqueios frequentes;
- › Surgimento de mensagens de *pop-up*, imagens, sons estranhos ou aplicações instaladas sem consentimento;
- › Desactivação espontânea de mecanismos de protecção, como os antivírus;
- › Incapacidade do sistema de reconhecer vogais acentuadas;
- › Actividade constante e inexplicável da ligação à Internet;
- › Alteração da página inicial ou do motor de busca favorito;
- › Redireccionamento constante para páginas estranhas na Internet;
- › Surgimento de novos favoritos ou barras de ferramentas no seu *browser*;
- › Publicação de comentários em redes sociais;
- › Estabelecimento de conversas em ferramentas de *Instant Messaging* (*Skype*, *Google Talk*, etc.);
- › Múltiplas devoluções de *e-mails*, por falha na recepção, que o utente não reconhece como tendo sido enviados por si;
- › Surgimentos do ícone do *Java* na barra de tarefas, sem que esteja a executar nenhuma aplicação baseada nesta tecnologia.

6.3. Como identificar sinais de furto de identidade

Os efeitos do furto de identidade podem ser mais nefastos se não forem detectados o mais cedo possível. Daí a importância de o/a utente conhecer formas de se poder aperceber de que está a ser vítima de furto de identidade, de modo a ser capaz de conter os seus efeitos. Vejamos, então, algumas estratégias de detecção atempada deste fenómeno.

Para detectar o furto de identidade atempadamente, o/a utente deve:

- › Permanecer alerta quanto a actividade estranha na conta de *e-mail* e nos perfis das redes sociais;
- › Manter uma vigilância constante sobre todas as contas – contas bancárias, de investimento e cartões de crédito:
 - » Verificar se recebe e conferir os extractos mensais com as últimas operações realizadas;
 - » Procurar atentamente por operações não efectuadas por si;

6. PREVENÇÃO

- › Contactar a instituição financeira caso não receba os extractos mensais;
- › Subscrever os alertas de actividade que as empresas financeiras com quem trabalhar oferecerem;
- › Investigar qualquer recusa de crédito – pode ser um sinal de que houve furto de identidade e utilização indevida da conta;
- › Se os seus extractos de conta estiverem a ser enviados para um endereço que não o seu, informar o representante da instituição de que a mudança de endereço não foi autorizada e que alguém pode estar a usar ilicitamente a conta; nesta situação é fulcral pedir cópias de todos os extractos de conta e uma lista das operações efectuadas desde o último extracto.

7.

CONTENÇÃO

[illegible]

7. CONTENÇÃO

7.1. Infecção por *malware*

Em caso de infecção por *malware*, o utente deve:

- › Desligar o computador da rede, de modo a que não possa infectar mais nenhum computador;
- › Proceder à limpeza do computador: a limpeza pode implicar a reinstalação de todo o sistema e pode ser feita pela vítima, caso esta tenha conhecimentos concretos dos procedimentos, ou por um especialista;
- › Optando pela desinfecção, fazer correr a ferramenta de limpeza através do “Modo de Segurança” ou a partir de um CD ou *pen-drive* com um antivírus que tenha vindo de um computador não infectado;
- › Alterar todas as palavras-passe.

7.2. Furto de identidade

Após ser vítima de furto de identidade através da Internet, o utente necessita de conhecer os meios que possui para conter os efeitos do crime e para suavizar o impacto deste na sua vida pessoal, social e financeira.

Em caso de furto de identidade o utente deve:

- › Contactar a sua instituição financeira imediatamente, se esta lhe indicar actividades de conta anormais ou se for informado/a sobre dívidas que não contraiu;
- › Cancelar os cartões de crédito e de débito, pedir a emissão de novos cartões e alterar os códigos PIN caso o cibercriminoso possa ter tido acesso às respectivas contas ou a estes dados;
- › Fechar as contas a que o cibercriminoso possa ter tido acesso ou que tenha aberto;
- › Cancelar o acesso ao *homebanking* e pedir novos códigos caso o cibercriminoso possa ter tido acesso a este serviço;
- › Pedir à instituição em causa para disponibilizar os formulários necessários para contestar que as acções levadas a cabo pelo criminoso tenham sido praticadas pela vítima;
- › Não existindo formulários específicos, contestar por carta para o endereço que a instituição financeira indicar;
- › Aferir junto do banco da possibilidade de obter a restituição do dinheiro;

7. CONTENÇÃO

- › Pedir todos os extractos de contas e relatórios dos cartões de crédito e débito, procurar erros e operações não efectuadas por si, informar as instituições financeiras caso se depare com alguma e contestar a autoria das acções criminosas;
- › Se encontrar erros, lançar alerta de fraude no relatório do cartão de crédito;
- › Solicitar à instituição financeira que impeça que os dados constantes do relatório de crédito estejam disponíveis;
- › Observar atentamente o relatório do cartão de crédito nos anos seguintes ao furto de identidade;
- › Verificar se existe alguma responsabilidade de crédito assumida com a sua identidade na central de responsabilidades de crédito do Banco de Portugal;
- › Fazer queixa junto do Ministério Público, da Polícia Judiciária, da Polícia de Segurança Pública ou da Guarda Nacional Republicana;
- › Apresentar às instituições financeiras o comprovativo da queixa apresentada;
- › Obter o registo criminal e verificar se a informação está correcta;
- › Alterar a palavra-passe de acesso à sua conta de *e-mail* caso o cibercriminoso possa ter tido acesso a esta;
- › Cancelar os documentos de identificação caso o cibercriminoso tenha tido acesso aos mesmos;
- › Notificar as companhias prestadoras de serviços com quem trabalha, a estação dos correios mais perto do domicílio, a Segurança Social e o IMTT;
- › Avisar a entidade empregadora de que se foi vítima de furto de identidade, para o caso de se depararem com informações incorrectas sobre a vítima;
- › Guardar todos os *e-mails*, SMS, cartas ou qualquer registo de comunicações quer entre si e o autor do crime ou suspeito quer entre si e a instituição financeira, para que sirvam de prova, se necessário.

Em caso de furto de identidade para difamação na rede social *Facebook*:

1. Se o autor do crime criar um perfil falso da vítima para publicar conteúdos difamatórios, a vítima deve proceder da seguinte forma, usando o *Facebook*:
 - › Denunciar a conta; para isso a vítima deve:
 - » Clicar na opção “...” ao lado do botão “Mensagem” no canto superior direito do perfil da conta em causa;
 - » Aparecerão, então, quatro opções e deve seleccionar-se a opção “Denunciar”;
 - » De seguida seleccionar a opção “Denunciar esta conta”;

7. CONTENÇÃO

- » Surgirá a mensagem “O que está errado com esta conta?”, momento em que se deverá clicar na opção “Esta cronologia está a fazer-se passar por mim ou por alguém que conheço”;
- » Imediatamente surgirá no ecrã a pergunta “Está a fazer-se passar por quem?” ao que a vítima deverá clicar na alternativa “Eu”;
- » Surgirá esta mensagem “Com base no que escolheste, aqui estão algumas coisas que podes fazer.” e então deverá seleccionar-se a opção “Enviar para o *Facebook* para revisão”
- » Finalmente deverá clicar-se na opção “Concluído”.

› Denunciar o conteúdo publicado; para isso a vítima deve:

- » Clicar na seta direccionada para baixo localizada no canto superior direito das publicações e seleccionar a opção “Não gosto desta publicação”.

2. Se o autor criar uma página falsa em nome da vítima para publicar conteúdos difamatórios:

› Denunciar a página e o conteúdo publicado; para isso a vítima deve:

- » Clicar na opção “...” ao lado do botão “Mensagem” no canto superior direito da página em causa;
- » Aparecerão então cinco opções e deve seleccionar-se a opção “Denunciar Página”
- » De seguida a vítima deve seleccionar a opção “Está a perturbar-me ou a alguém que conheço”;
- » Surgirá, então, esta mensagem “Lamentamos que tenhas passado por esta experiência. Aqui estão algumas coisas que podes tentar para resolver isto.”, momento em que se deverá seleccionar a opção “Enviar para o Facebook para revisão”
- » Finalmente deverá clicar-se na opção “Concluído”.

3. Se o autor do crime utilizar o perfil verdadeiro da vítima para publicar conteúdos difamatórios:

› Mudar a palavra-passe de acesso; para isso a vítima deve:

- » Carregar no ícone com um cadeado no canto superior direito da barra azul no topo da página;

7. CONTENÇÃO

- » De seguida seleccionar a opção “Ver mais definições”;
 - » Posteriormente a vítima deverá clicar na opção “Geral” no canto superior esquerdo da página que surge;
 - » Surgirão, então, no ecrã as “Definições gerais de conta” e na opção “Palavra-passe” a vítima deverá clicar em “Editar”
 - » De seguida, a vítima deverá inserir a antiga palavra-passe e a nova duas vezes,
 - » Posteriormente deverá seleccionar a opção “Guardar alterações”;
 - » De seguida aparecerá a seguinte mensagem “A tua palavra-passe foi alterada. Terminar sessão em outros dispositivos?” e deverá clicar-se na opção “Terminar a minha sessão em outros dispositivos”
 - » Finalmente, a vítima deverá clicar em “Enviar”.
- › Apagar os conteúdos publicados; para isso a vítima deve:
 - » Clicar na seta direccionada para baixo localizada no canto superior direito das publicações e seleccionar a opção “Eliminar”;
 - » De seguida aparecerá a seguinte mensagem “Tens a certeza de que queres eliminar isto?”, devendo a vítima seleccionar a opção “Eliminar” novamente.

4. Em qualquer dos casos:

- › Bloquear o autor do crime, para que a pessoa deixe de ter acesso à informação que a vítima publica, assim como, todos os utilizadores do *Facebook* que constituam um incómodo; para isso a vítima deve:
 - » Clicar na opção “...” ao lado do botão “Mensagem” no canto superior direito do perfil do utilizador que quer bloquear;
 - » Aparecerão então quatro opções e deve seleccionar-se a opção “Bloquear”;
 - » De seguida, surgirá esta mensagem “Tens a certeza de que queres bloquear ...?” “ao que a vítima deverá seleccionar a opção “Confirmar”.
- › Fazer queixa junto do Ministério Público, da Polícia Judiciária, da Polícia de Segurança Pública ou da Guarda Nacional Republicana.

ANEXOS

[illegible]

ANEXOS

Glossário

Bots e botnets – O termo *bot* é uma abreviatura de *robot*. Os criminosos distribuem *software* malicioso (*malware*) que pode transformar o computador do utilizador num *bot* (robô) ou zombie, como também pode ser designado. Quando tal acontece, o computador do utilizador pode executar tarefas automatizadas através da Internet, sem o seu conhecimento. Os criminosos utilizam normalmente *bots* para infectar um grande número de computadores. Estes computadores formam uma rede ou uma *botnet*. Os criminosos utilizam as *botnets* para enviar mensagens de *spam*, disseminar vírus, atacar computadores e servidores e cometer outros tipos de crimes e fraudes. Se o computador do utilizador fizer parte de uma *botnet*, pode tornar-se lento e inadvertidamente o utilizador pode estar a ajudar os criminosos;

Browser – Programa para aceder à Internet e que já vem por definição no computador;

Chat – Conversa online;

Cookies – Um *cookie* é um ficheiro criado por um *site* para armazenar informações no computador do utilizador, nomeadamente as preferências deste quando visita esse *site*. Quando se visita um *site* que utiliza *cookies*, o *site* pode pedir ao *browser* instalado no computador para colocar um ou mais *cookies* no disco rígido do computador do utilizador. Mais tarde, quando este regressa ao *site*, o *browser* enviará os *cookies* que pertencem a esse *site*. Isto permite que o *site* apresente informação dimensionada às necessidades dos seus utilizadores. Existem *cookies* que os *sites* criam para que o utilizador não precise de introduzir a sua palavra-passe quando visitar o *site* uma segunda vez, por exemplo. Outros *sites* utilizam *cookies* para guardar as preferências do utilizador;

Dados informáticos – Qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

Dados de tráfego – Dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

Download – Transferência de conteúdos da Internet para o equipamento do utilizador;

E-mail – Mensagem de correio electrónico;

Flash – Arquivos gerados pelo *Adobe Flash Player*, que é um *software* utilizado geralmente para a criação de animações interactivas;

Fornecedor de serviço – qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores;

Java – Linguagem de programação;

Link – Ligação a sítio da Internet;

ANEXOS

Login – Processo através do qual o acesso a um sistema informático é controlado através da identificação e autenticação do utilizador através de credenciais fornecidas por esse mesmo utilizador;

Malware – É um *software* destinado a infiltrar-se em sistemas de computadores alheios de forma ilícita, com o intuito de causar danos, alterações ou furto de informações (confidenciais ou não). Vírus de computador, *worms*, e *spywares* são considerados *malwares*;

Pop-ups – Janela extra que abre no *browser* ao visitar uma página *web* ou ao abrir uma ligação específica;

Sistema informático – Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção; a definição de sistema informático de acordo com a CCCE abrange todas as formas de tecnologia que vão além dos sistemas tradicionais de computadores de grande porte ou área de trabalho, tais como telefones móveis modernos, *smartphones*, *PDAs*, *tablets* ou similares;

Spoofing – Um ataque de *spoofing* corresponde a uma situação em que uma pessoa ou programa consegue passar por outra/o através da falsificação de dados e disfarçando a sua verdadeira identidade, ganhando assim uma vantagem ilegítima;

Spyware – Programa automático de computador que recolhe informações sobre o utilizador e sobre os seus hábitos na Internet e transmite essa informação a uma entidade externa, sem o conhecimento e consentimento do usuário. O *spyware* pode ser desenvolvido por empresas, que desejam monitorizar os hábitos dos utilizadores e fazer publicidade adaptada aos seus interesses, procurando vender os seus produtos pela Internet. Por outro lado, muitos vírus transportam *spyware*, que visa furtar certos dados confidenciais dos utilizadores, como dados bancários;

Website/Site – Sítio da Internet ou página da *Web*;

Wi-fi – Ligação sem fios à Internet;

World Wide Web/WWW/Web – Termo da língua inglesa que, em português, se traduz literalmente por “teia mundial”; é um sistema de documentos em hipermédia que são interligados e executados na Internet.

Contactos de apoio das instituições bancárias associadas à
Associação Portuguesa de Bancos

Banco BIG 707 244 707	Banif 808 200 200	Caixa Geral de Depósitos 707 24 24 24
Banco do Brasil 707 222 500	Barclays 707 50 50 50	Deutsche Bank 808 201 251
Banco Carregosa Porto - 22 608 64 64 Lisboa - 21 013 41 00	BBVA 707 256 256	Millennium 707 50 24 24
Banco Finantia 707 788 080	BNP Paribas 21 791 02 00	Montepio 808 20 26 26
Banco Invest 800 200 160	BPI 707 020 500	Novo Banco 707 247 365
Banco Popular 808 20 16 16	Caixa Agrícola 808 20 60 60	Santander 707 21 24 24

[illegible]

[illegible]

