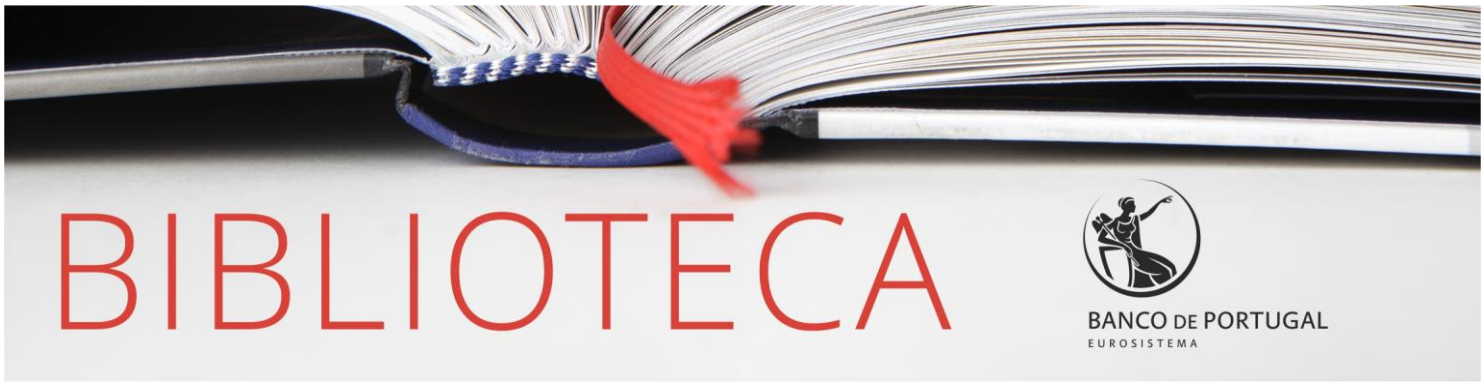


BIBLIOTECA

BANCO DE PORTUGAL
EUROSISTEMA

Newsletter Biblioteca • Publicação trimestral • n.º 3 • ano VIII • julho 2015

Bibliotema

Privacidade na Internet

Gostava que alguém utilizasse as suas Credenciais para fazer algo em seu nome?

E se qualquer pessoa souber em cada momento o que está a fazer?

E se os seus dados pessoais forem divulgados ao público?

A privacidade é o direito à reserva de informações pessoais e da própria vida privada que todos os cidadãos devem ter e pode ser entendida como o direito de controlar a exposição e disponibilidade dos seus dados.

Nesta matéria encontram-se duas leis de referência, embora esteja em aprovação o Regulamento Comunitário de Proteção de Dados que se prevê que venha a vigorar a partir de 2016 ou 2017:

- Lei n.º 67/98, Lei da Proteção de Dados Pessoais

Definindo dados pessoais: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

- Lei n.º 46/2012, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas

Esta lei é pioneira ao introduzir, no setor das comunicações eletrónicas, a obrigação de notificação, à Comissão Nacional de Proteção de Dados (CNPD), de violações de dados pessoais, definidas na lei como "violações da segurança que provoquem, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público."

Quando a violação de dados for suscetível de afetar negativamente dados pessoais do utilizador, as empresas devem ainda, notificar os mesmos para que possam tomar as precauções necessárias. A lei presume que uma violação de dados afeta negativamente o utilizador sempre que possa resultar em usurpação de identidade, danos físicos, humilhação ou danos de reputação.

Índice

Bibliotema • Privacidade na Internet | 1 · 5

Destaques | 8

Novos recursos de informação | 9 · 11

Análise de recursos eletrónicos | 12

Está prevista para 2016 a entrada em vigor do novo regime jurídico da proteção de dados na Europa, apresentando algumas alterações significativas às leis atualmente em vigor. Sendo um regulamento a nível europeu acaba com a discrepância legislativa relativamente a este tema na Europa, apresenta-se exigente ao nível de coimas a aplicar bastante acima das que se praticam hoje e determinará uma maior responsabilização das empresas em geral no que diz respeito à proteção de dados pessoais.

Para mais informações sobre a regulamentação e como agir consulte a página da Comissão Nacional de Proteção de Dados (CNPD).

Com o aparecimento das redes sociais, as pessoas passaram a abdicar livremente da sua privacidade, partilhando com o mundo, a sua localização, os seus interesses, relações pessoais e profissionais. Cada vez que criamos uma conta de e-mail ou rede social, limitamo-nos a aceitar políticas de privacidade que nem sequer lemos (muitas vezes nem abrimos). Não sabemos quem pode ter acesso à nossa informação e como é que ela pode ser utilizada.

Cuidados a ter nos acessos à Internet

- Não partilhe informações online que não gostaria de tornar públicas. Mantenha confidenciais os seus números de conta, nomes de utilizador e palavras passe.
- Perceba o que o mundo digital sabe sobre si. Pesquise em diversos motores de busca (Google, Yahoo, Ask, Bing, etc.) por si próprio (pesquise por primeiro e último nome), inclua na pesquisa a secção de imagens. Faça a avaliação das informações encontradas e, se a informação não for pública ou não a quer expor, procure o contacto do website e solicite a sua remoção.
- A política de privacidade de qualquer website deve explicar claramente quais os dados que recolhe sobre si, o modo como são protegidos, partilhados e utilizados. Se o website que habitualmente consulta não tem declaração de privacidade então não o utilize.
- Reveja com regularidade o que outros escrevem sobre si. Peça aos seus "amigos" para não publicarem informação sobre si, salvo se for explicitamente autorizado.
- Partilhe o seu endereço de correio eletrónico ou nome de utilizador apenas com pessoas ou organizações de confiança.
- Utilize passwords fortes e mude-as regularmente. Não use a mesma password para todos os acessos (banca online, correio eletrónico, website de viagens, jogos, etc.).
- Antes de fornecer os seus dados pessoais em formulários de registo, leia atentamente as instruções e forneça apenas a informação necessária (em geral identificada como obrigatória).
- Dropbox, SkyDrive, CloudPT, Google Drive, entre outros, são conhecidos como soluções para partilha e armazenamento de informação. Este conjunto de serviços existentes na internet, não tendo localização fixa e, em muitos casos, estando distribuídos por servidores com localizações distintas, estão sujeitos a leis diversas e a informação fica disponível aos prestadores destes serviços e a atacantes que os comprometam. Sempre que utilize estes serviços, encripte os seus ficheiros de modo a assegurar que eles só serão acessíveis por si e por alguém a quem confia essa informação.
- Mantenha o seu computador atualizado com as últimas versões de software, incluindo antivírus e mantenha ativada uma firewall.
- Tenha atenção a oportunidades de negócio demasiado aliciantes, anúncios falsos, pedidos de auxílio com transferências de fundos, prémios maravilhosos. Lembre-se de verificar a veracidade do que lhe está a ser apresentado e se tem qualquer dúvida desista pois pode estar a ser vítima de fraude.

A toda a hora. Em todo o lugar. Na ponta dos dedos!

Com a proliferação dos equipamentos móveis, estes são cada vez mais uma presença regular no nosso dia-a-dia. Andam sempre connosco, seja em casa, na escola, no trabalho, em viagem de negócios ou em lazer. São crescentes as capacidades de armazenamento e processamento. São inúmeras as circunstâncias em que recorremos ao smartphone ou ao tablet. Seja equipamento pessoal ou empresarial, mantemos a nossa ligação não só com os elementos da nossa lista de contactos mas com o mundo, através de uma conexão de dados ou wireless. Nas cidades, nos centros comerciais, nos restaurantes, nos transportes públicos, nos estabelecimentos de ensino, no nosso local de trabalho, até mesmo no nosso prédio (disponibilizado por um vizinho benemérito ou

distraído), são cada vez mais os pontos de acesso à internet onde podemos conectar facilmente o nosso dispositivo. Configuramos contas de correio eletrónico. Navegamos na Internet. Transferimos ficheiros mais ou menos confidenciais. Podemos armazenar tarefas ou notas de reuniões. Instalamos jogos e diversas aplicações. Registamos fotograficamente momentos que partilhamos de imediato nas redes sociais ou simplesmente arquivamos no cartão de memória ou enviamos para a "nuvem".

Usamos cada vez mais os dispositivos móveis como extensões ou substitutos dos nossos computadores de secretária ou portáteis, tanto a nível pessoal como profissional.

Atrai-nos esta facilidade de acesso a toda a hora em todo o lugar.

Com o avanço tecnológico dos dispositivos móveis, nomeadamente no que diz respeito a smartphones e tablets, o volume de transferência de dados produzido por estes equipamentos tem vindo a crescer exponencialmente. O custo associado ao consumo de dados móveis torna especialmente apetecível a utilização de redes sem fios (WiFi) de acesso livre, ou grátis, quando existente. Esta prática pode, no entanto, representar um custo indireto, no que diz respeito à proteção de dados pessoais e/ou corporativos se for utilizada uma rede sem fios insegura.

Proteção de dispositivos móveis

Para proteger o seu equipamento móvel e a informação que ele contém, descrevem-se abaixo algumas dicas, fáceis de por em prática e com retorno garantido.

Além do PIN do Cartão, defina um código para bloqueio de ecrã

Dificulta o acesso ao conteúdo do equipamento.

Proteger o dispositivo com um PIN para ligar/desligar dispositivo.

Definir um PIN para bloquear o ecrã, após alguns segundos/minutos sem atividade.

Evite utilizar sequências de teclado, por exemplo, 1234, 6789, 1111.

Evite senhas como o seu nome, data de nascimento, marca do carro, dados que facilmente alguém relaciona.

Use senhas longas e alfanuméricas, sempre que possível.

Instale Apps e Jogos somente de fontes confiáveis tais como as disponibilizadas em lojas oficiais (Apple Store, Play Store, Market)

Não clique em alertas de publicidade e outras ligações via SMS, Email ou Redes Sociais

Atenção às hiperligações que recebe via SMS, MMS, Email, Facebook, Twitter, entre outros.

Clicar numa destas ligações pode instalar código malicioso no seu dispositivo permitindo que alguém mal intencionado aceda remotamente ao seu dispositivo e às informações pessoais e profissionais guardadas no dispositivo, sem que se aperceba do que está acontecer.

Se desejar mesmo uma aplicação cujo link recebeu, aceda à loja de Apps do seu dispositivo e procure pela versão fidedigna.

Instale e mantenha atualizado uma App Antivírus

Tenha cuidado com os falsos antivírus.

Se lhe aparece um alerta de um antivírus que não tem ou não se lembra de ter instalado, a informar que o seu smartphone está infetado e que para ser limpo basta clicar nessa mensagem, desconfie. Esta mensagem em si é que pode ser o vírus!

Desbloqueio ilegal de equipamentos

Não use dispositivos ilegalmente desbloqueados – Jailbreaked (iOS) ou Rooted (Android).

Compromete segurança do dispositivo, além de violar disposições legais e garantia.

Reponha definições de fábrica

Se adquirir um telemóvel que tenha sido usado previamente por outra pessoa, reponha as definições de fábrica para garantir que, embora usado, o sistema foi limpo de definições pessoais. Encontra facilmente esta opção nas definições do seu equipamento.

Armazenamento, Backup e Transferência de Dados

Seja cuidadoso quanto aos dados que armazena no seu equipamento móvel. Muitos equipamentos já permitem encriptação nativa do dispositivo. Não perde funcionalidade. Ganha segurança em caso de perda ou roubo de informação.

Atenção à sincronização automática de conteúdos do telemóvel para a nuvem. Mesmo sem saber poderá estar a fazê-lo. Verifique nas definições do seu equipamento. Lembra-se dos últimos acontecimentos com fotografias de celebridades que circularam na Internet?

Faça regularmente uma cópia de segurança dos seus contactos, fotografias, vídeos e restantes dados.

Quando viajar, pense no seu equipamento móvel

Verifique junto do seu operador móvel os termos do serviço de Roaming.

Dependendo da situação, pondere adquirir um cartão de voz e dados temporários no país de destino. Poderá tornar-se mais económico.

Ao ligar-se a redes WiFi não deverá ter custos adicionais, contudo certifique-se que o faz com segurança.

O que fazer em caso de Roubo ou Extravio do equipamento

Informe a sua empresa caso tenha informações e contas de correio definidas no equipamento.

Altere as passwords e outros códigos que possam eventualmente estar armazenados no dispositivos, por exemplo, login automático em contas de email, aplicações, etc..

Configure se possível o dispositivo para apagar os dados após um número de tentativas sem sucesso, mensagem de alerta, aumento volume, aviso operadora e bloqueio do número. Ativar a localização remota, se suportado pelo seu equipamento.

Tipos de Redes sem fios

Tipicamente, existem dois tipos de redes WiFi que podem ser acessíveis. As redes Ad-Hoc e as redes típicas via access point. As primeiras caracterizam-se por ligações ponto-a-ponto ligando equipamentos diretamente entre si. São exemplo as redes de Hotspot pessoais, em que um telefone funciona como ponto de acesso à Internet e vários equipamentos podem-se ligar através do mesmo, ligando-se por WiFi.

O segundo tipo são as tradicionais redes em que é disponibilizado um ponto de acesso, o típico "router wireless" em tudo semelhante à oferta comercial dos operadores de internet para o segmento doméstico.

Redes sem fios Inseguras

De um modo geral, é comumente entendível que uma rede sem fios insegura é aquela que não apresenta password ou credenciais para acesso. Nesse tipo de redes, basta aceder e imediatamente tem-se acesso à Internet. São redes que existem, tipicamente, em zonas públicas, tais como centros comerciais, aeroportos, hotéis e, mais recentemente, em zonas de lazer, restauração e transportes públicos. Por definição estas redes não são necessariamente inseguras, mas a realidade tem vindo a

provar que o acesso a estas redes deverá ser encarado com extrema cautela.

Seja por motivos relacionados com publicidade, com rastreio e avaliação de perfis de utilização da Internet ou com segurança, o exercício de algumas cautelas deverá ser uma prioridade máxima aquando da ligação a este tipo de redes. Imagine o leitor que está num café e decide aceder à sua página do Facebook, ou ler o seu email. O seu smartphone indica-lhe que existe uma rede sem fios grátis nas proximidades e a ligação é efetuada. A partir deste momento, o leitor começará a efetuar uma utilização normal da Internet e de forma grátis, sem a consciência de que por trás daquela rede sem fios poderão estar motores estatísticos para monitorizar consumos e hábitos ou até, no pior dos casos, um pirata informático a extrair dados sensíveis do equipamento, como por exemplo credenciais de acesso privado a contas de email, redes sociais ou até online Banking.

É possível, hoje em dia, uma pessoa com intuitos maliciosos, mascarar-se de HotSpot grátis, usando inclusive uma identificação de rede que seja familiar, sem que seja facilmente detetado, permitindo-lhe iludir os utilizadores, colocando-se "entre" o utilizador e a Internet, extraindo a totalidade da informação gerada pelo utilizador. Essa informação pode, posteriormente ser utilizada para fins impróprios.

Em boa verdade, são tantos os benefícios, como os riscos, ameaças e fragilidades que este novo paradigma de comunicação sempre presente nos traz.

Tal como aconteceu com a democratização dos computadores pessoais, também os smartphones e tablets são alvos cada vez mais apetecíveis para tentativas de acesso não autorizado, exploração de vulnerabilidades e códigos maliciosos/vírus. É seu principal intuito obter dados pessoais, informação privada (fotografias, passwords guardadas nos dispositivos, sites visitados, localização geográfica, SMS, registos de chamadas) ou relacionada com as responsabilidades profissionais de cada um - quantas vezes usámos já o nosso smartphone ou tablet para ler ou reencaminhar um email de trabalho, aceder a documentos ou tomar notas numa reunião?

A concentração de informação potencialmente útil num equipamento de reduzidas dimensões, a juntar à nula segurança física, fácil transporte, desvio e ocultação, são deveras um aliciante para indivíduos mal-intencionados. Se aos fatores anteriores incrementarmos o valor do equipamento em si, estaremos perante um risco tendencialmente crescente.

Aumente a segurança do acesso em redes WiFi

Nem tudo são más notícias, no entanto. Há um conjunto de medidas que o utilizador pode promover, no sentido de incrementar a confiança ou a segurança dos dados pessoais no acesso WiFi grátis. Deixamos algumas dicas:

• Garanta que o seu dispositivo móvel não está configurado para aceder automaticamente a redes abertas, sem credenciais;

• Evite a utilização de serviços importantes tais como online banking, reduzindo o acesso a tarefas básicas de browsing sem caráter pessoal ou informação sensível envolvida.

• Privilegie a utilização de HotSpots disponibilizados pelos operadores de acesso à Internet, tipicamente protegidos por credenciais;

• Privilegie a utilização de sítios cujo endereço comece por https, em detrimento de http. Embora não sejam garantia de segurança absoluta, são um considerável incremento de segurança. Este tipo de acesso é visível, normalmente, através de um ícone de um cadeado na barra de endereços do browser.

• Sempre que possível, ative os mecanismos de autenticação dupla para os serviços que o suportem. Com este mecanismo, além das credenciais de acesso típicas (nome de utilizador e password) existe um código específico que muda regularmente. Mesmo que alguém capture as suas credenciais de acesso, não terão o segundo código. Este tipo de mecanismos está presente em serviços comuns Google, Apple, Facebook, Twitter, LinkedIn, entre outros.

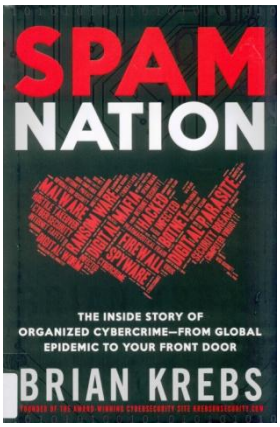
• A utilização de um serviço de VPN (Virtual Private Network), embora revestido de maior complexidade de configuração e nem sempre aplicável a todos os dispositivos móveis, é garantia de que os dados do utilizador são encriptados.

Bibliotema • Destaques

KREBS, Brian

Spam nation: the inside story of organized cybercrime: from global epidemic to your front door

Napperville, Il.: Sourcebooks, 2014. 251 p.
ISBN 978-1-4022-9561-4



Brian Krebs é jornalista, investigador e perito em segurança informática. Neste livro, acompanha algumas das maiores operações de s*pam* eletrónico e de pirataria informática que disseminam inúmeros vírus, ataques de *phishing* e de *spyware*, atingindo os consumidores de todo o mundo.

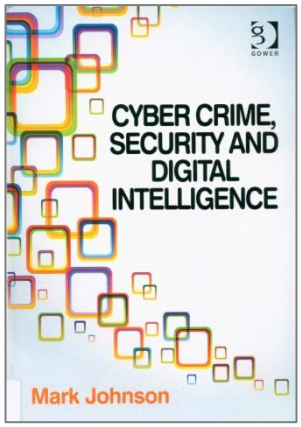
O autor utiliza diversas entrevistas, para dar a conhecer histórias de crime informático e para mostrar os perigos a que o utilizador comum se expõe, quando inconscientemente adota comportamentos de risco que são um convite para os "ladrões digitais". Disseca a atuação dos *spammers*, que podem não contaminar as nossas contas de *email*, mas recolhem informações pessoais, como o nome do utilizador e a *password*, que depois vendem no "mercado negro digital".

Depois de expor as fragilidades da segurança informática, Krebs propõe soluções concretas para proteger o consumidor *on-line* e para travar esta onda de crimes informáticos. Conclui com o reforço da ideia de que o comportamento do consumidor é tão importante como a utilização de antivírus e *firewall.*

JOHNSON, Mark

Cyber crime, security and digital intelligence

Farnham: Gower Publishing, 2013.252 p.
ISBN 978-1-4094-5449-6



"Cyber crime, security and digital intelligence" é uma obra de grande relevância no mundo da internet e redes informáticas da atualidade, especialmente porque o nosso modo de vida depende muito da economia digital, que é absolutamente dependente das tecnologias *online*. Neste livro, Mark Johnson descreve, em linguagem simples, a evolução do crime informático e a natureza das ameaças mais recentes, bem como as respostas dadas pela segurança informática e pela *digital intelligence* a estes desafios.

Aqueles cuja atividade económica depende da *web*, *email*, *skype* ou outras ferramentas de conexão precisam de trabalhar num ambiente digital em que possam confiar e sabem que os riscos da utilização da internet são elevados, principalmente porque o crime informático é cada vez mais sofisticado e ameaça a integridade e disponibilidade dos dados.

Este livro é de leitura obrigatória para informáticos, estudantes e todos os que utilizam a internet como ferramenta de trabalho. De acordo com o autor, decisões complacentes por parte dos governos e utilizadores desinformados podem conduzir ao fracasso da uma tecnologia, da qual depende a nossa economia e o nosso modo de vida.

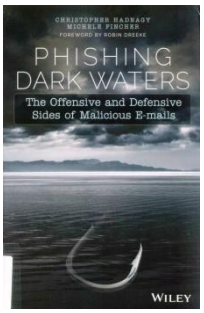
Bibliotema • Lista bibliográfica selecionada

Livros

HADNAGY, Christopher; FINCHER, Michele

Phishing dark waters: the offensive and defensive sides of malicious e-mails

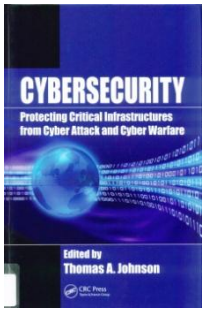
Indianapolis: Wiley, 2015. 192 p.
ISBN 978-1-118-95847-6



JOHNSON, Thomas A.

Cybersecurity: protecting critical infrastructures from cyber attack and cyber warfare

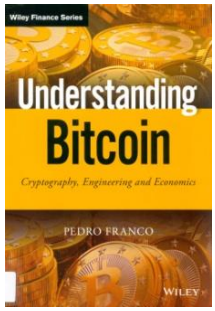
Boca Raton: CRC Press, 2015. 347 p.
ISBN 978-1-4822-3922-5



FRANCO, Pedro

Understanding Bitcoin: cryptography, engineering, and economics

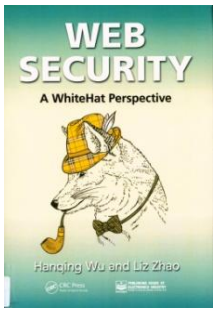
Chichester: Wiley, 2015. 268 p.
ISBN 978-1-119-01916-9



HANQUING, Wu; ZHAO, Liz

Web security: a whitehat perspective

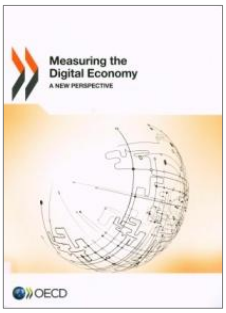
Boca Raton CRC, 2015. 508 p.
ISBN 978-1-4665-9261-2



OCDE

Measuring the digital economy: a new perspective

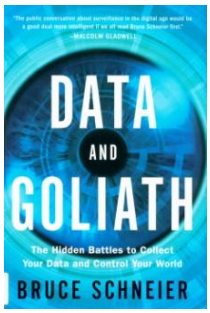
Paris: OCDE, 2014. 156 p.
ISBN 978-92-64-21130-8



SCHNEIER, Bruce

Data and Goliath: the hidden battles to collect your data and control your world

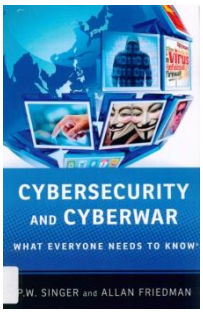
New York: W. W. Norton, 2015. 383 p.
ISBN 978-0-393-24481-6



SINGER, Peter Warren; FRIEDMAN, Allan

Cybersecurity and cyberwar: what everyone needs to know

Oxford: Oxford University Press, 2014. 306 p.
ISBN 978-0-19-991811-9



VENÂNCIO, Pedro Dias

Lei do cibercrime: anotada e comentada

Coimbra: Coimbra Editora; Lisboa: Wolters Kluwer Portugal, 2011. 361 p.
ISBN 978-972-32-1906-7

Artigos

CAMPBELL, Alexander

Cyber risk special report

"Operational Risk & Regulation" Mar 2015. v. 15, n. 2, p. 19-27

SHOEMAKER, Dan

The NICE framework: why you need to understand this important initiative

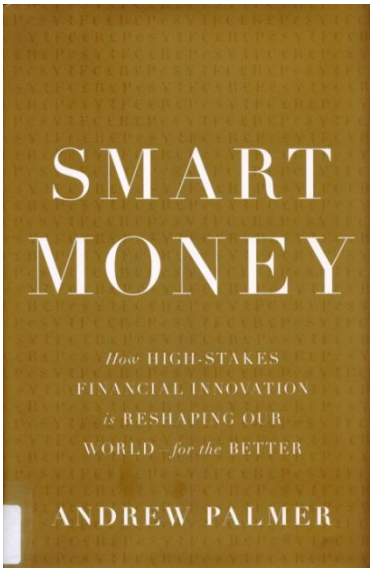
"EDPACS" 2015. v.51, n. 6, p.1-7

YELSHYNA, Aliaksandra; ANDRADE, Francisco

Um ambiente inteligente de resolução de litígios: repercussões jurídicas na privacidade e proteção de dados

"Scientia Ivridica" jan-abr 2015. t. LXIV, n. 337, p. 111-134

Novidades • Destaques



Palmer, Andrew

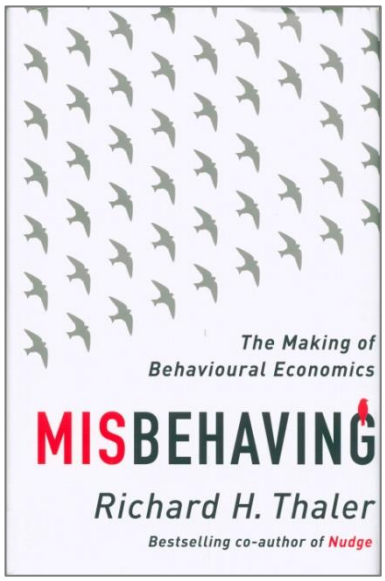
Smart money: how high-stakes financial innovation is reshaping our world for the better

New York: Basic Books, 2015. 285 p.
ISBN 978-0-465-06472-4

Este livro nasceu a partir de uma reportagem sobre inovação financeira, publicada na revista "The Economist" em 2012. O autor visita diversos centros financeiros no âmbito de uma investigação que lhe permitiu alterar a ideia que a indústria financeira é apenas a indústria dos grandes bónus, negócios imprudentes, ganância, enriquecimento dos banqueiros e destruição das poupanças das pessoas.

Palmer aborda a história da inovação financeira, que é também a história dos avanços humanos. As primeiras formas de financiamento serviram para satisfazer necessidades muito básicas, de comércio, proteção e crédito. Ao longo de séculos a complexidade das sociedades e da tecnologia cresceu em paralelo com a indústria financeira.

O autor reabilita a imagem da indústria financeira e apresenta ao leitor inovações financeiras, tais como "peer-to-peer lending" ou "crowdfunding", nas quais os grandes bancos não apostam, mas que estão a financiar muitos empreendedores e a aumentar o bem-estar na nossa sociedade.



THALER, Richard H.

Misbehaving: how economics became behavioural

London: Allen Lane, 2015. 415 p.
ISBN 978-1-846-14403-5

Este livro aborda o impacto dos fatores emocionais, sociais e psicológicos nas decisões económicas dos indivíduos. Tradicionalmente, pressupõe-se que as escolhas económicas são sempre racionais, o que não corresponde à verdade. A abordagem da economia comportamental defendida por Richard Thaler sustenta que os seres humanos estão no centro da economia e que, como humanos que são, são propensos a errar e portanto a desviar-se dos padrões de racionalidade tomados como corretos.

O autor recheia o livro de casos que cruzam a economia com a psicologia, com implicações profundas e até divertidas. Por exemplo, quando o mercado entra numa situação de "bolha especulativa", porque é que os investidores não tomam a decisão racional de contribuir para que os preços voltem à situação inicial? A resposta sai fora dos parâmetros da racionalidade. Os investidores preferem ganhar mais dinheiro, alimentando a bolha e esperam poder sair mais depressa do que os outros.

Thaler revela como a análise económica comportamental contribui para alargar os nossos horizontes, levando-nos a compreender as tomadas de decisão dos agentes económicos.

Novos recursos de informação

ADMATI, Anat; HELLWIG, Martin

Os banqueiros vão nus: o que está mal na banca e como o corrigir

Lisboa: Gradiva 2015. 497 p.
ISBN 978-989-616-632-8

AGUIAR, Maria Margarida Corrêa de

Pensões: um novo contrato social para reconciliar as gerações

Lisboa: Bnomics, 2015. 205 p.
ISBN 978-989-713-134-9

ALVES, Filipe; SARMENTO, António

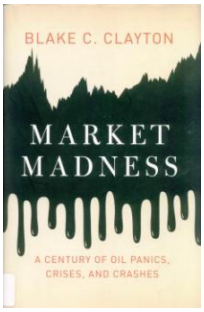
Os novos donos disto tudo

Lisboa: Matéria-Prima Edições, 2015. 197 p.
ISBN 978-989-769-012-9

CEDIPRE – Centro de Estudos de Direito Público e Regulação

Estudos de regulação pública – II

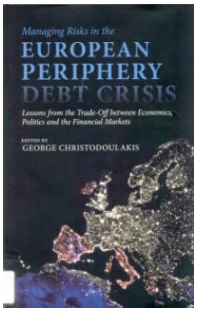
Coimbra: Coimbra Editora, 2015. 540 p.
ISBN 978-972-32-2336-1



CLAYTON, Blake C.

Market madness: a century of oil panics, crises, and crashes

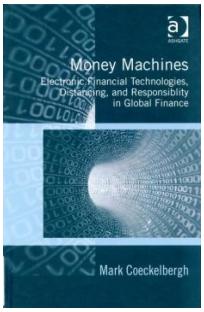
Oxford: Oxford University Press, 2015. 221 p.
ISBN 978-0-19-99905-4



CHRISTODOULAKIS, George

Managing risks in the European periphery debt crisis: lessons from the trade-off between economics, politics and the financial markets

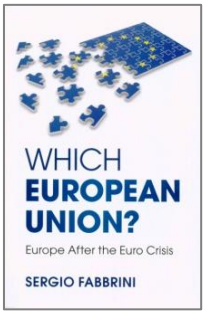
Basingstoke: Palgrave Macmillan, 2015. 275 p.
ISBN 978-1-137-30494-0



COECKELBERGH, Mark

Money machines: electronic financial technologies, distancing, and responsibility in global finance

Farnham: Ashgate Publishing, 2015. 204 p.
ISBN 978-1-4724-4508-7

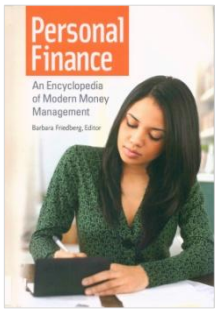


FABRINI, Sergio

Which European Union? Europe after the euro crisis

Cambridge: Cambridge University Press, 2015. 338 p.
ISBN 978-1-107-50397-7

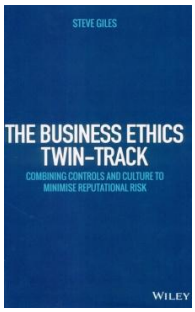
Novos recursos de informação



FRIEDBERG, Barbara

Personal finance: an encyclopedia of modern money management

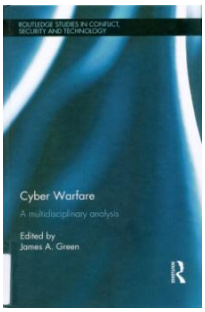
Santa Barbara: Greenwood, 2015. 403 p.
ISBN 978-1-4408-3031-0



GILES, Steve

The business ethics twin-track: combining controls and culture to minimize reputational risk

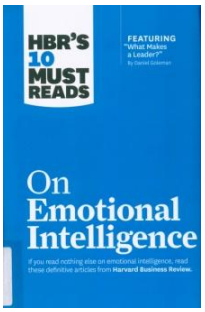
Chichester: Wiley, 2015. 302 p.
ISBN 978-1-118-78537-9



GREEN, James A.

Cyber warfare: a multidisciplinary analysis

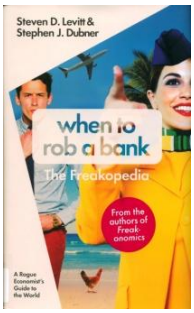
Abingdon: Routledge Taylor and Francis Group, 2015. 182 p.
ISBN 978-1-138-79307-1



HARVARD BUSINESS REVIEW

HBR's 10 must reads on emotional intelligence

Boston: HARVARD BUSINESS REVIEW PRESS, 2015. 208 p.
ISBN 978-1-63369-019-6



LEVITT, Steven D.; DUBNER, Stephen J.

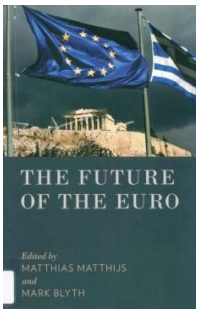
When to rob a bank: a Rogue Economist's guide to the world

London: Allen Lane, 2015. 387 p.
ISBN 978-0-141-98096-6

LYONS, Gerard

O consolo da economia: como todos iremos beneficiar com a nova ordem mundial

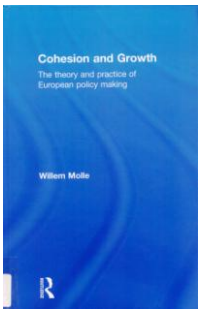
Lisboa: Círculo de Leitores, 2015. 493 p.
ISBN 978-989-644-322-1



MATTHIJS, Matthias; BLYTH, Mark

The future of the euro

New York: Oxford University Press, 2015. 399 p.
ISBN 978-0-19-023324-2



MOLLE, Willem

Cohesion and growth: the theory and practice of European policy making

London: Routledge, 2015. 342 p.
ISBN 978-1-138-84662-3

Novos recursos de informação

RODRIGUES, Maria de Lurdes; SILVA, Pedro Adão

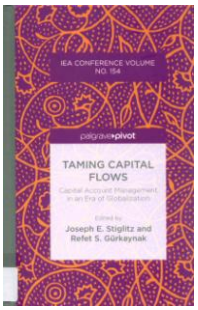
Governar com a Troika: políticas em tempo de austeridade

Coimbra: Almedina, 2015.
798 p.
ISBN 978-972-40-6081-1

SANTOS, Sofia

A banca tem coração? As práticas de gestão necessárias para os bancos do futuro

Lisboa: BNOMICS, 2015. 126 p.
ISBN 978-989-713-143-1



STIGLITZ, Joseph; GURKAYNAK, Refet S.

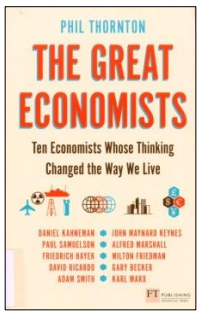
Taming capital flows: capital account management in an era of globalization

London: Palgrave, 2015. 216 p.
ISBN 978-1-137-42766-3

STIGLITZ, Joseph; KALDOR, Mary

Em busca de segurança: proteção sem protecionismo e o desafio da governança global

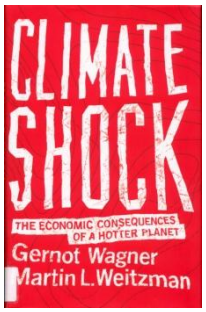
Lisboa: Bertrand Editora, 2015.
559 p.
ISBN 978-972-25-2888



THORNTON, Phill

The great economists: ten economists whose thinking changed the way we live

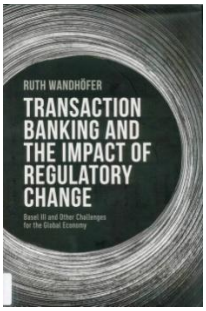
Harlow: Pearson Education, 2014. 249 p.
ISBN 978-1-292-00941-4



WAGNER, Gernot; WEITZMAN, Martin

Climate shock: the economic consequences of a hotter planet

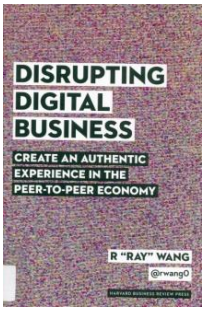
Princeton: Princeton University Press, 2015. 250 p.
ISBN 978-0-694-15947-8



WANDHÖFER, RUTH

Transaction banking and the impact of regulatory change: Basel III and other challenges for the global economy

Basingstoke: Palgrave Macmillan, 2014. 285 p.
ISBN 978-1-137-35176-0



WANG, Ray

Disrupting digital business: create an authentic experience in the peer-to-peer economy

Boston: Harvard Business Review Press, 2015
ISBN 978-1-4221-4201-1

Análise de recursos eletrónicos

European Union Agency for Network and Information Security

http://www.enisa.europa.eu/

A ENISA é a Agência da União Europeia para a Segurança das Redes e da Informação. Trabalha para as instituições da União Europeia e Estados-Membros e tem como objetivo promover as melhores práticas e conhecimentos na área de segurança Informática.

Através da página do ENISA podemos explorar a secção "Critical Infrastructure Protection" (CIIP), responsável por auxiliar as agências pertencentes à União Europeia a implementar e desenvolver estratégias de resposta às ameaças a infraestruturas ou informações críticas. A CIIIP realiza exercícios para responder a ataques informáticos, faz a análise do impacto dos ataques informáticos em serviços críticos e analisa as consequências que estes crimes podem ter para o bem-estar social.

A secção "Risk Management " é responsável pela compilação de um conjunto de normas necessárias para reportar incidentes ao nível da segurança. Aqui podemos encontrar guias técnicos e especificações de medidas de segurança. A agência avalia a capacidade de resposta das redes de informação, verifica e reforça as normas de *compliance* e audita procedimentos.

A segurança das redes de informação tem uma importância vital para o bem-estar dos cidadãos e o bom funcionamento das empresas da União Europeia que utilizam tecnologias como banda larga, serviços bancários online, comércio eletrónico, e dispositivos móveis.

Investopedia

http://www.investopedia.com/

Criada em 1999, a página da *Investopedia* encontra-se focada na formação e educação financeira, disponibilizando para tal informação e recursos nessa área. Detentora de um dicionário dedicado a termos financeiros, a *Investopedia* oferece diversos recursos de aprendizagem tais como simuladores e tutoriais, divididos por várias categorias (*Active Trading*, *Forex,* Opções, Futuros, etc.). Contém também informação específica acerca de investimentos, finanças pessoais, *trading* e mercados.

Através da *Investopedia* é possível acompanhar os artigos e notícias da atualidade financeira, os diferentes mercados e os conselhos dos seus *financial advisors.* Os artigos são agrupados por diferentes temas tendo em conta as categorias de finanças pessoais, investimentos, estratégias de *trading* entre outras.

Adicionalmente, dispõe de recursos específicos de preparação para exames como o CFA (*Chartered Financial Analyst*), vídeos explicativos e calculadoras de auxílio para diversos cálculos financeiros (conversor de moeda, anuidades, futuros, etc.).

Biblioteca

Mais de 70 000 monografias

Mais de 1500 títulos de periódicos

Recursos eletrónicos

Relatórios e contas

Instruções do Banco de Portugal

Legislação nacional e comunitária

Coleção de obras impressas entre os sécs. XVII e XIX

Obras editadas pelo Banco de Portugal

Pesquisas efetuadas por especialistas

Acesso à Internet

Sala de Leitura

R. Francisco Ribeiro, 2

1150-165 Lisboa

Entrada livre

De 2.ª a 6.ª feira

9h00 – 16h30

(entrada até às 15h30)

T +351 213 130 626

F + 351 213 128 116

biblioteca@bportugal.pt

NEWSLETTER BIBLIOTECA • Banco de Portugal Av. Almirante Reis, 71 | 1150-012 Lisboa • www.bportugal.pt • Edição Departamento de Serviços de Apoio | Núcleo de Documentação e Biblioteca • Design Departamento de Serviços e Apoio | Documentação, Edição e Museu | Serviço de Edições e Publicações • Lisboa, 2015