# GUIA PRÁTICO DE SEGURANÇA DE TI PARA PEQUENAS EMPRESAS

*Como ter a certeza de que a sua empresa tem proteção de segurança abrangente de TI*

#protectmybiz

KASPERSKY lab

*Há pequenas empresas de muitos tamanhos e feitios. Porém, no mundo de hoje, nenhuma organização pode correr o risco de ignorar a segurança online – quer seja uma equipa que trabalhe num escritório ou um indivíduo que trabalhe a partir de casa. É um problema que afeta toda a gente.*

Embora o cibercrime chame a atenção das manchetes, normalmente as vítimas são as multinacionais ou o governo. Mas, sem sombra de dúvida, os casos menores são a maior história.

Só em 2014, foram detetados 143 milhões de novos casos.[1] E a maioria diz respeito a indivíduos e organizações que não se consideravam possíveis alvos.

Na realidade, qualquer pessoa é um alvo. A boa notícia é que há uma enorme diferença entre ser um alvo e ser uma vítima.

Na maioria dos casos resume-se simplesmente a estar preparado. É por isso que elaborámos este guia: para o ensinar a manter o seu negócio seguro.

## O QUE É O MALWARE?

O termo malware refere-se a programas informáticos concebidos para fins maliciosos. Costuma atacar dispositivos sem o conhecimento do utilizador. A Kaspersky Lab é uma empresa líder mundial na deteção de malware, tendo recebido um maior número de melhores classificações do que qualquer outro fornecedor de segurança.[2]

## POR QUE MOTIVO NECESSITO DE PROTEÇÃO?

Os cibercriminosos não têm de retirar todo o dinheiro da sua conta bancária para que isso represente um impacto significativo na sua empresa. As interrupções causadas por malware podem afetar a sua produtividade e fluxo de caixa, causando uma cadeia de efeitos indesejáveis. Uma vez que pode proteger-se contra estas eventualidades através de passos relativamente simples, não é preciso muito para ter paz de espírito.

1. Testes AV
2. Estudo dos resultados de testes independentes TOP3 de 2014

# A SUA LISTA DE VERIFICAÇÃO DE SEGURANÇA

**O PRIMEIRO PASSO PARA PROTEGER A SUA EMPRESA É ANALISAR COMO TRABALHA E VER ONDE PODE REDUZIR O RISCO. POR ISSO, FAÇA UMA RÁPIDA VERIFICAÇÃO DE INTEGRIDADE DE TI NA SUA EMPRESA:**

## PROTEÇÃO ANTI-MALWARE ✔

À semelhança do seguro empresarial, quando se trata de produtos que protegem a sua empresa, o objetivo é obter o melhor que conseguir. Se ainda não possui software de elevada capacidade que proteja os seus dispositivos contra infeções, deve fazer com que seja uma prioridade.

Infelizmente, estar apenas vigilante online não é suficiente. Todos nós sabemos que não devemos abrir anexos de remetentes desconhecidos ou transferir documentos de sites suspeitos, mas a verdade é que muitas infeções vêm de fontes fiáveis que foram comprometidas.

## COMPORTAMENTOS DE NAVEGAÇÃO ✔

Educar a sua equipa sobre a importância das respetivas ações online pode evitar-lhe muitos problemas. Esperamos que os seus colaboradores compreendam que existem determinados tipos de sites que não devem visitar no trabalho. Porém, se utilizarem dispositivos móveis (como smartphones ou tablets) para uso pessoal, depois de saírem do edifício, podem estar menos conscientes dos riscos para a segurança. Portanto, é boa ideia bloquear sites inadequados para garantir que ficam inacessíveis aos computadores de trabalho. Aumentar a consciência geral para as ameaças de segurança de TI também ajuda os funcionários a permanecerem seguros na utilização pessoal.


### ? COMO PODE AFETAR-ME?

Nunca recebeu um e-mail de um amigo ou familiar que contenha uma ligação interessante, que, uma vez aberta, parecia suspeita? Assim que um malware infeta um computador, pode executar ações sem o conhecimento do utilizador. É por isso que as fontes fiáveis nem sempre são de confiança.

## PALAVRAS-PASSE ✔

Os funcionários também devem certificar-se de que utilizam palavras-passe únicas e seguras que incluam símbolos, números e letras maiúsculas e minúsculas. A descodificação de palavras-passe por programas que efetuam uma análise simples em dicionários até encontrarem a adequada ocorre todos os dias. E mesmo que seja segura, se uma palavra-passe comprometida for utilizada para vários fins, isso pode dar origem a uma violação ainda maior.

## ATUALIZAÇÕES ✔

São detetados quatro novos programas de malware a cada segundo.[3] Tem de se manter à frente. Isto significa utilizar atualizações automáticas para melhorar o seu software de segurança todos os dias, atualizando todo o outro software sempre que possível - e certificar-se de que todas as pessoas na sua empresa fazem o mesmo. Lembre-se, os programas que não tenham sido atualizados são o principal meio utilizado pelos cibercriminosos para aceder às empresas.

## CERTIFIQUE-SE DE QUE NÃO COMETE NENHUM DOS SEGUINTES ERROS CLÁSSICOS DE PALAVRA-PASSE:

1. Escolher opções fáceis de memorizar e adivinhar, como "palavra-passe" ou "123456"
2. Utilizar como palavra-passe o seu endereço de e-mail, nome ou outros dados que podem ser facilmente obtidos
3. Definir perguntas de lembretes de palavra-passe que um hacker possa responder com uma simples pesquisa - por exemplo, o nome de solteira da sua mãe
4. Fazer ligeiras modificações óbvias para palavras comuns, como, por exemplo, colocar um "1" no final
5. Utilizar frases comuns. Até pequenas frases como "amote" são facilmente descobertas


*Para obter mais sugestões sobre como criar palavras-passe difíceis de descodificar, consulte as nossas publicações no blogue sobre o assunto.*

3 Testes AV

EM 2014

**295 500**

NOVAS AMEAÇAS DE MALWARE MÓVEL[4]

## SERVIÇOS BANCÁRIOS ✔

Desde o redirecionamento para versões falsas de sites fiáveis, à utilização de malware para espionar a sua atividade, os cibercriminosos dispõem de vários métodos para obter as suas informações financeiras. Tem de tomar medidas ativas para impedi-los.

Esteja atento às tentativas de "phishing" utilizadas pelos burlões para se fazerem passar pelo seu banco: utilize sempre um browser seguro e certifique-se de que verifica atentamente o URL antes de introduzir os seus dados pessoais em qualquer site. Além disso, é melhor evitar a introdução de tais informações em e-mails, porque podem ser acedidas por pessoas que não são de confiança.

## DISPOSITIVOS MÓVEIS ✔

Como trabalhar em viagem faz agora parte do nosso quotidiano, o cibercrime está cada vez mais direcionado para os dispositivos móveis. Em 2014, 295 500 novas ameaças de malware móvel (criadas especificamente para smartphones e tablets) foram detetadas todos os meses. [5] Embora seja tão importante proteger os telemóveis como os tablets, Mac ou PC, apenas 32% das pequenas empresas reconhece atualmente o risco apresentado pelos dispositivos móveis.[6]

## ENCRIPTAÇÃO ✔

Se tiver dados confidenciais armazenados nos seus computadores, estes devem ser encriptados, para que não possam ser utilizados se forem perdidos ou roubados. É importante ter noção que, como empresa, as informações que detém são um bem muito valioso, que tem de ser protegido.

## ? O QUE É O PHISHING?

"Phishing" é um método utilizado pelos cibercriminosos para fazerem passar-se por uma instituição fiável, na esperança de obter informações - por exemplo, palavras-passe e informações de cartão de crédito - que possam usar para defraudá-lo.

4 & 5 De acordo com a Kaspersky Lab
6 Inquérito global de riscos de segurança de TI de 2014

# COMPREENSÃO DOS RISCOS

**É MUITO FÁCIL FALAR SOBRE CIBERSEGURANÇA, MAS PARA A MAIORIA DE NÓS, POR VEZES É DIFÍCIL COMPREENDER DO QUE SE TRATA. CONFRONTAR A REALIDADE DESSES PROBLEMAS DA FORMA MAIS DIFÍCIL NÃO É, CERTAMENTE, O QUE TODOS PRETENDEM. POR ISSO, TENTÁMOS FAZER COM QUE SEJA MAIS FÁCIL ATRAVÉS DE ALGUNS EXEMPLOS, AS RESPETIVAS CONSEQUÊNCIAS E COMO PODERIAM SER EVITADAS.**

## *Uma chávena de café muito cara*

Depois de despedir-se do último cliente do dia, Thomas deixa que seja o seu colega a fechar o escritório. Há um café mesmo à frente do escritório, onde combinou encontrar-se com um amigo. Ao lembrar-se que o pagamento a um dos fornecedores estava agendado para o dia seguinte, decidiu tratar do assunto na altura, para não se esquecer.

Utilizou o computador portátil para estabelecer ligação à rede Wi-Fi do restaurante, iniciou sessão no Website do banco onde tem uma conta e fez a transferência. Satisfeito por se ter lembrado do que tinha para fazer, aconchegou-se na cadeira e saboreou o café.

Quando pediu a conta, verificou que não tinha dinheiro. Enquanto tentava perceber o que se passara, os empregados do café aguardavam pelo pagamento.

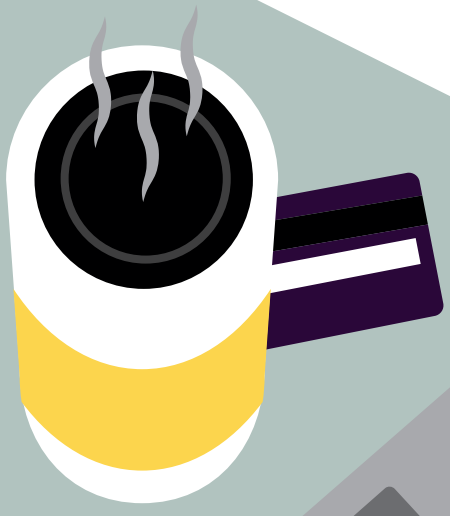
### COMO É QUE ACONTECEU?

Infelizmente, não havia qualquer tipo de anti-malware instalado e um programa de keylogging malicioso acedeu ao computador. O responsável por esse programa recebeu um registo de todas as informações inseridas por si. E, como estava a utilizar Wi-Fi pública desprotegida, havia também o risco de interceção dos dados da transação.

### O QUE PODERIA TER FEITO?

Os serviços bancários devem ser utilizados apenas em dispositivos que possuam anti-malware instalado, e sempre através de um browser seguro. Com a funcionalidade Dinheiro Seguro da Kaspersky, o Thomas poderia ter toda a certeza de que a transação seria segura.

É importante notar que, uma vez que ele estava a utilizar uma rede pública não protegida, os dados que estava a transmitir seriam muito mais fáceis de intercetar do que se utilizasse uma ligação privada. Porém, se tivesse a funcionalidade Dinheiro Seguro instalada, poderia tirar proveito da comodidade dos serviços bancários online sem ter motivos de preocupação.



# *Correio cada vez menos bem-vindo*

Maria é psicóloga e todas as manhãs abre o e-mail na Web para verificar quando está confirmado o seu próximo compromisso. No topo da caixa de entrada, verifica que tem uma mensagem de uma rede social que utiliza, a solicitar-lhe para atualizar a palavra-passe para algo mais seguro. Clica na ligação fornecida, confirma a palavra-passe existente e cria uma nova palavra-passe substituindo letra sim letra não por um asterisco.

Satisfeita com o facto de o acesso à conta ser mais difícil, volta para a caixa de entrada e rapidamente se esquece do sucedido...

...até que recebe uma carta de chantagistas a ameaçarem-na de que vão publicar os dados de cada um dos clientes que recorrem aos seus serviços de terapia.

## COMO É QUE ACONTECEU?

Maria foi vítima de um esquema de phishing. Apesar de o website parecer igual ao que visitou milhares de vezes, era apenas uma cópia falsa. Depois de terem acedido aos detalhes do perfil de Maria, tiveram também acesso aos detalhes sobre a sua atividade. Tentaram utilizar a mesma palavra-passe que conseguiram obter para ter acesso ao e-mail de trabalho dela. E como já a tinha utilizado para ambas as contas, eles conseguiram ler todas as mensagens e os ficheiros anexados a eles – um dos quais era uma lista completa dos clientes e respetivos dados de contacto.

## O QUE PODERIA TER FEITO DE MANEIRA DIFERENTE?

Em primeiro lugar, deveria ter noção que as organizações e os websites legítimos não pedem detalhes por e-mail. Uma vez que ela já tinha clicado na ligação, com um bom software de segurança instalado já tinha sido alertada para o facto de que o website era falso.

O outro erro foi utilizar a mesma palavra-passe para atividades profissionais e pessoais.

# PORQUÊ ESCOLHER A KASPERSKY

**ESFORÇAMO-NOS PARA PROPORCIONAR A PROTEÇÃO MAIS EFICAZ, RÁPIDA E EFICIENTE CONTRA CIBERAMEAÇAS. NO KASPERSKY SMALL OFFICE SECURITY, PERSONALIZÁMOS ESSA EXPERIÊNCIA NUMA SOLUÇÃO TÃO UTILIZÁVEL COMO ÚTIL. PARA QUE POSSA CONTINUAR A TRABALHAR NO QUE FAZ MELHOR - GERIR A SUA EMPRESA.**

Compreendemos que, no que respeita à cibersegurança, as pequenas empresas estão numa posição ideal. Enfrentam muitas das ameaças às empresas e têm muitas das vulnerabilidades dos utilizadores domésticos. Pensamos que esta posição única merece uma abordagem especial à segurança.

Reembalar um produto para o consumidor como uma solução para pequenas empresas não é a melhor opção. Por exemplo, não oferece proteção para os servidores, mas muitas pequenas empresas utilizam este sistema ou irão fazê-lo em breve. Ao contrário dos utilizadores domésticos, as empresas têm de proteger vários dispositivos facilmente.

No entanto, retirar as funções de uma solução destinada a grandes empresas também não funciona. As pequenas empresas não têm equipas de TI específicas ou tempo para lidar com software complicado concebido para especialistas.

O Kaspersky Small Office Security foi concebido para ser abrangente, sem ser complicado - para que possa ter paz de espírito, sem que a segurança consuma demasiados recursos. Não vai ocupar-lhe demasiado tempo e abrange uma ampla gama de dispositivos, para que possa ficar protegido seja qual for o seu negócio.

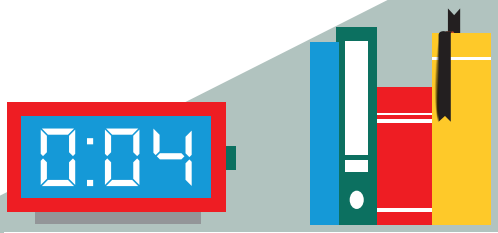
## ? POR QUE MOTIVO NÃO TENHO PROTEÇÃO GRATUITA?

Embora haja soluções de segurança gratuitas, estas não proporcionam uma proteção abrangente. Na verdade, fazem-no de propósito. É assim que encorajam os utilizadores a atualizar para uma versão paga.

Quando a sua empresa está em risco, necessita que a proteção seja a melhor possível - permanentemente.

# FAZER ISSO ACONTECER

**AGORA QUE IDENTIFICÁMOS AS ÁREAS QUE DEVEM SER TIDAS EM CONTA COMO PARTE DA SUA POLÍTICA DE SEGURANÇA, ESTÁ NA ALTURA DE CONSIDERAR - COM A AJUDA DE UMA SOLUÇÃO PERSONALIZADA - COMO PODE IMPLEMENTÁ-LA.**




## VERIFICAR QUE AS ATUALIZAÇÕES OCORREM REGULARMENTE

No que respeita ao Kaspersky Small Office Security, não tem de preocupar-se. Vamos atualizar automaticamente a sua proteção em tempo real, mantendo-o informado sobre novas ameaças à medida que vão surgindo.


## APLICAR PALAVRAS-PASSE SEGURAS

Utilize o Kaspersky Password Manager para facilitar a tarefa aos seus funcionários. Esta funcionalidade gera automaticamente palavras-passe seguras e armazena-as numa base de dados encriptada. Desta forma, só terão de memorizar uma palavra-passe principal e estará muito mais seguro.

## ENCRIPTAR E FAZER CÓPIAS DE SEGURANÇA DOS DADOS CRÍTICOS/CONFIDENCIAIS

Com o Kaspersky Small Office Security, é fácil armazenar informações importantes em "cofres" encriptados. Além disso, com a função de restauro, mesmo que os computadores ou servidores bloqueiem, os dados vitais não são perdidos.

## INCLUIR TODOS OS SEUS DISPOSITIVOS

O Kaspersky Small Office Security oferece proteção para os tablets e smartphones suportados. E se os dispositivos forem perdidos ou roubados, pode ajudá-lo a localizá-los e a apagar, de maneira remota, todas as informações confidenciais.

## BLOQUEAR OS MALFEITORES

A nossa premiada funcionalidade Dinheiro Seguro pode ser ativada com apenas alguns cliques e permite uma navegação supersegura. Ao utilizá-la para verificar se os websites com os quais está a interagir não estão comprometidos, poderá de imediato impedir a probabilidade de uma violação. Entretanto, as nossas funções de anti-malware, anti-spam e firewall mantêm as portas fechadas aos criminosos durante a restante atividade online.

# PROTEJA A SUA EMPRESA AGORA.

Criado para responder às exigências únicas das empresas mais pequenas, o Kaspersky Small Office Security combina proteção avançada com facilidade de utilização, essencial para empresas como a sua.

Visite **kaspersky.com/pt/protectmybusiness** e descubra como o Kaspersky Small Office Security pode proteger a sua empresa.

**PROTEJA A SUA EMPRESA AGORA**

## JUNTE-SE À CONVERSA

*#protectmybiz*


Veja-nos no YouTube

Goste no Facebook

Visite o nosso blogue

Siga-nos no Twitter

Junte-se a nós no LinkedIn

Saiba mais em kaspersky.com/pt/protectmybusiness

## ACERCA DA KASPERSKY LAB

A Kaspersky Lab é o maior fornecedor privado do mundo de soluções de proteção de terminais. A empresa encontra-se classificada entre os quatro principais fornecedores de soluções de segurança para utilizadores de terminais a nível mundial*. Ao longo dos seus mais de 17 anos de história, a Kaspersky Lab foi sempre uma inovadora na segurança de TI e fornece soluções de segurança digital eficientes para grandes empresas, PME e consumidores. A Kaspersky Lab, cuja sociedade gestora de participações sociais está registada no Reino Unido, opera atualmente em quase 200 países e territórios por todo o mundo, oferecendo proteção a mais de 400 milhões de utilizadores. Saiba mais em www.kaspersky.pt.

* Em 2013, a empresa ocupava o quarto lugar na classificação IDC de Worldwide Endpoint Security Revenue by Vendor. A classificação foi publicada no relatório IDC "Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares" (IDC #250210, agosto de 2014). O relatório classificava os fornecedores de software consoante as suas receitas em vendas de soluções de segurança de terminais em 2013.