**O que é malware**

Malware (abreviatura para “software malicioso”) é considerado um tipo de software irritante ou malígno que pretende acessar secretamente um dispositivo sem o conhecimento do usuário. Os tipos de malware incluem spyware, adware, phishing, vírus, Cavalos de Tróia, worms, rootkits, ramsoware e sequestradores de navegador.

**De onde vem um malware**

Malware geralmente acessa o seu dispositivo através da internet e via e-mail, embora ele possa fazer isso através de sites hackeados, demos de games, arquivos de música, barras de ferramentas, software, assinaturas gratuitas ou qualquer outra coisa que você baixa na internet.

**Como reconhecer um malware**

Um computador lento é geralmente um sinal de que a sua máquina pode ter sido infectada com malware, assim como pop-us, spam e panes frequentes.

**Como remover um malware**

A melhor maneira de se livrar de um malware e facilmente removê-lo é através do uso de ferramentas de remoção, como encontradas em um bom software de antivírus. Avast Antivirus pode rapidamente e facilmente remover qualquer malware de seus dispositivos.

**Como se prevenir de um malware**

Não abra anexos de e-mails que vêm de fontes desconhecidas ou inesperadas.

**Antivírus**

E como surgiu o antivírus?

Em 1983 Fred Cohen desenvolveu um vírus experimental para apresentar um seminário sobre segurança da computação, foi ele que designou o termo “vírus” para esse tipo de software. Até hoje ele é conhecido como o “pai do vírus de computador”. Em 1989 foi criado o vírus que criptografava (protegia com senha) os seus dados do seu computador, e eles só eram devolvidos mediante um pagamento. Aí em 1990 a Norton lançou seu antivírus que protegia o computador de vírus polimórficos (são vírus que fazem modificações cada vez que infecciona um novo computador).

Como funciona um antivírus?

Esse programa obedece alguns comandos para detectar softwares mal intencionados. O primeiro é a atualização, todo dia novos vírus são encontrados, quando são descobertos a empresa responsável pelo software decodifica ele e manda como atualização via internet, assim se o antivírus perceber algum código parecido em seu computador, ele move direto para quarentena (esse termo é usado para dizer que esse arquivo está funcionando livremente, mas está em observação). O segundo passo é analisar todos os programas que estão sento executados. Depois ele faz uma busca algoritmia (ele abre o programa e lê os códigos que os constituí) se ele encontrar algum código que já está em seu banco de dados, então ele coloca o programa em quarentena. E a checagem que é a varredura, o antivírus esporadicamente faz uma varredura em todos os arquivos, comparando os códigos dos programas com armazenados em seu banco de dados, caso encontre algum dado suspeito, ele coloca em quarentena!

**Avast**

As raízes da Avast remontam a 1988, quando os pesquisadores tchecos Eduard Kučera e Pavel Baudiš encontraram o vírus de Vienna e empreenderam a missão de salvar os computadores do mundo de vírus como esse e outros.

Hoje, Avast tem mais de 500 profissionais sediados em Praga, República Tcheca, com escritórios adicionais em Alemanha, EUA e China, parceiros de distribuição em todos os mercados, e uma comunidade global de entusiastas Avast.

**AVG**

A história começou em 1991, quando Jan Gritzbach e Tomas Hofer, fundaram a empresa Girosft, na cidade de Brno na República Checa. O primeiro produto da nova empresa foi o antivírus AVG (abreviação de Anti-Virus Guard), lançado em 1992 no mercado local. Em 1997, as primeiras licenças do AVG foram vendidas na Alemanha e no Reino Unido e, em 1998, o AVG foi lançado nos Estados Unidos.

Em 1999, a empresa resolveu adotar uma estratégia ousada que mudaria seu furuto: fornecer de graça o antivírus para tornar-se popular mundialmente. Com este lema, um dos fundadores da AVG, Jan Gritzbach, decidiu que preferiria dar o software a ficar para sempre desconhecido e, por conseqüência, não vender nada. O que alguns gurus poderiam taxar como loucura, de fato, funcionou. A empresa viu seu número de usuários aumentar extraordinariamente ano a ano. A marca ganhou visibilidade e, de quebra, o tão sonhado faturamento. Em 2001, Jan Gritzbach decidiu vender a empresa para o fundo de investimento Benson Oak Capital Acquisitions (com sede na República Theca). Quatro anos depois, o Benson Oak valorizou seu investimento, vendendo 65% da empresa para a Intel Capital e Enterprise Investors (fundo de private equity com sede na Polônia) por US$ 52 milhões.

**Norton**

Norton Antivirus foi desenvolvido originalmente por Peter Norton , que dirigia uma empresa de software de computador chamado Peter Norton Computing Co. Em 1990 , a Symantec comprou a empresa de Norton, incluindo os direitos de todo o software que ele desenvolveu . Um programa em particular, foi um programa antivírus baseado em DOS , que mais tarde se tornaria a base para o Norton Antivirus em distribuição hoje.   
Características

Norton Antivirus tem várias características , mas o seu objectivo primário ( como o próprio nome sugere ) é fazer a varredura em busca de vírus , arquivos de quarentena e excluir esses arquivos que não pode salvar. Além de verificar a existência de vírus e excluí-los, Norton Antivirus também tem a opção de ativar o que chama a função "Auto -Protect" . Este recurso permite que o usuário simplesmente ir sobre seu negócio normal do computador , enquanto o Auto - Protect verifica cada e-mail , faça o download e arquivo para garantir que nenhum ganho de software malicioso uma posição no computador.

Um problema com o Norton Antivirus é que ele ocupa uma enorme quantidade de recursos do computador , a fim de fazer seu trabalho. Mesmo quando o programa não está digitalizando ativamente em busca de vírus, o programa ocupa uma grande quantidade de memória e velocidade de processamento , efetivamente retardando o computador enquanto ele trabalha .

## Dicas de proteção

Muita gente pensa que basta ter um antivírus no computador para estar livre de malwares. De fato, esse tipo de software cumpre um papel muito importante, mas nem mesmo a melhor solução consegue ser 100% eficaz. A arma mais poderosa, portanto, é a prevenção. Eis algumas dicas simples, mas essenciais para isso:

* Aplique as atualizações do sistema operacional e sempre use versões mais recentes dos softwares instalados nele;
* Tome cuidado com anexos e link em e-mails, mensagens instantâneas e redes sociais, mesmo quando a mensagem vier de pessoas conhecidas;
* Antes de baixar programas desconhecidos, busque mais informações sobre ele em mecanismos de buscas ou em sites especializados em downloads;
* Tome cuidado com os sites que visita. É muito comum, por exemplo, a propagação de malwares em páginas de conteúdo adulto;
* Ao instalar um antivírus, certifique-se de que este é atualizado regularmente, do contrário, o programa não será capaz de identificar novos vírus ou variações de pragas já existentes;
* Faça uma varredura com o antivírus periodicamente no computador todo. Também utilize a ferramenta para verificar arquivos baixados;
* Vírus também podem ser espalhar por [cartões SD](http://www.infowester.com/sd.php), pendrives e aparelhos semelhantes, portanto, sempre verifique o conteúdo dos dispositivos removíveis e, se possível, não utilize-os em computadores públicos (faculdade, escola, lan house, etc).

**Celular**

**Diferenças entre infecções de computadores e de smartphones**

Nos computadores, os programas são executados em diferentes níveis de seguranças dentro de camadas de atividades. Os mais importantes rodam em ambientes mais seguros e menos acessíveis do sistema operacional, já os menos essenciais ficam em um local mais exposto e sujeito à alterações. É justamente na camada mais vulnerável que grande parte dos malwares começam a ser executados, podendo enviar cópias e estender suas ações a outros aplicativos, também situados neste grau de segurança. Já os programas mais agressivos conseguem burlar os níveis de segurança do sistema e se enraizar nas camadas importantes podendo comprometer o desempenho do computador e colocar em risco todo o seu funcionamento. Enquanto isso, o processo de infecção é bastante diferente nos smartphones. Os sistemas Android e iOS possuem arquitetura com somente duas camadas: uma mais restrita, com as principais execuções e os apps nativos do sistema, e outra onde estão as informações, arquivos e programas baixados pelo usuário. Quando um malware infecta um smartphone, suas ações irão se restringir ao nível mais exposto, limitando-se aos dados dos usuários e, raramente, tendo acesso às funções vitais do sistema. Porém, aparelhos desbloqueados via *jailbreak* ou *root* aumentam o risco de que *malwares*, mesmo inofensivos, comprometam as funções essenciais do sistema.

**Como acontecem as infecções?**

Atualmente, para contaminar seu smartphone com estas “pragas digitais” basta estar conectado à internet ou receber arquivos maliciosos por transmissões via bluetooth, SMS. Qualquer método que receba dados de outro aparelho é uma porta de entrada para estes programas danosos. A maneira mais segura para se utilizar o celular ainda é no “Modo Offline”. Grande parte dos malwares para celulares encontram-se nas próprias lojas oficiais de aplicativos, como a Google Play. No entanto, um relatório recente mostrou que essas ameaças começaram a circular via spams. Alguns desses programas, uma vez baixados, roubam seus dados e alteram configurações do sistema, com a possibilidade de enviar cópias de si mesmo ou de outros malwares por diferentes meios de transmissão de dados.

**As consequências de um smartphone infectado**

Um dos primeiros sintomas da presença de um malware, tanto em smartphones quanto computadores, é o comprometimento do desempenho do sistema. Devido às operações desses aplicativos nocivos, o processamento de dados do sistema passa a ter um maior gasto de memória, o que acaba por deixar o sistema mais lento, propenso a erros e congelamentos. Outro indício de “contágio” é o aumento significativo da transmissão de dados pela rede, além do envio de SMS, MMS, e-mails e outras mensagens pela internet sem o conhecimento dos usuários. Essas duas características são comportamentos padrões de malwares. Como foram desenvolvidos para roubar e transmitir dados, sejam eles imagens, contatos, relatórios de navegação na web e até informações bancárias, esses softwares acabam comprometendo o funcionamento de seu smartphone. Malware mais nocivos, no entanto, podem atrapalhar a performance do seu celular, interromper ou impedir ligações, podendo ainda contaminar outros aparelhos. Esses apps maliciosos são capazes também de transmitir mensagens, executar aplicativos, destruir o sistema operacional, aumentar o consumo da bateria de seu aparelho e até danificar o hardware.

**Como se prevenir?**

A primeira coisa a ser feita para manter o celular a salvo de aplicativos nocivos é estar atento aos dados enviados e recebidos pelo aparelho. Procure se assegurar sempre se os downloads tem uma procedência segura, observando comentários sobre comportamentos suspeitos e reclamações. Os malwares também pode estar camuflado em vídeos, músicas, aplicativos e fotos enviadas por e-mails, SMS, MMS e em transmissões via Bluetooth. Portanto, confirme o conteúdo com a pessoa que lhe enviou o arquivo, antes de abri-lo. Além desses cuidados, é bom ter em seu smartphone um bom antivírus para garantir que seu sistema está seguro e evitar futuras infecções. Nas lojas de aplicativos online, há uma boa quantidade de diferentes antivírus gratuitos, que poderão ser muito uteis na proteção de seu aparelho.

Fique atento aos sites que visita, pois, caso seu celular não tenha um antivírus ou firewall, você estará mais sujeito a infecções por pequenos malwares que poderão abri portas para softwares mais perigosos. Lembre-se de agendar varreduras periódicas com os antivírus instalados em seu aparelho. Isso pode evitar o aparecimento de pequenos erros e impedir instalações que possam camuflar infecções mais sérias.

Como os smartphones são dispositivos desenvolvidos para transmitir e receber informações de forma intensa, estes aparelhos se tornaram ambientes muito mais vulneráveis a vírus e malwares do que os computadores. Por isso, mantenha-se informado a respeito de novos tipos de infecções e sobre o funcionamento de seu smartphone. Caso seu celular esteja apresentando algum comportamento suspeito, instale ou troque seu antivírus e, se o problema continuar, leve-o a assistência técnica.

1.É muito fácil pegar um vírus para o seu celular

Podemos dizer que qualquer aparelho conectado à internet, seja ele o seu computador, o seu celular ou até mesmo estes eletrodomésticos que podem ser controlados via rede, está sujeito à ação de vírus. A diferença entre os sistemas também não é relevante: Android, iOS, Blackberry, Windows e os demais podem igualmente ser alvos de malware extremamente prejudiciais. Apesar deste problema, não é tão fácil assim pegar um vírus para o seu celular, já que todos os sistemas são relativamente seguros. Definitivamente, seu smartphone só será infectado se você baixar e dar permissões amplas para um aplicativo suspeito, o que não é a situação mais simples do mundo.

2.Quais são as principais formas de ameaça?

A ameaça mais básica para o seu celular são malwares dedicados a roubar informação e se valer da sua identidade para mandar spams, comprar produtos, serviços e outros problemas semelhantes. Normalmente eles se disfarçam na forma de aplicativos úteis, versões gratuitas de softwares pagos com linhas de código alterada. Apesar disso, é muito raro que eles consigam passar o crivo das lojas oficiais como o Google Play e a App Store. As empresas responsáveis por estes sistemas dedicam muito tempo e esforço para manter sua oferta de aplicativos livres deste tipo de esquema, ainda que a Google tenha mais dificuldade neste front graças à natureza livre do seu OS. Outros tipos de vírus que afetam celulares, ainda que sejam mais incomuns aqui no Brasil, são aqueles oriundos de SMS. Eles ocorrem quando você recebe uma mensagem com anexos, uma imagem ou outra coisa que precise ser aberta, e este arquivo em questão pode ser um tipo de malware. Mesmo quando você conhece quem enviou a mensagem, isso não torna o arquivo mais seguro, já que, uma vez dentro do seu aparelho, ele ganha acesso aos seus privilégios e sua lista de contatos, podendo enviar mensagens para todos os seus conhecidos. As consequências destes ataques normalmente são contas de telefone bem mais infladas, já que você acaba enviando SMS para serviços Premium que cobram para responder e enviar mensagens para o seu aparelho. Por essa razão esse tipo de ataque é tão infrequente no Brasil. Outras ameaças existem, como baseband hacking, processo no qual é possível escutar as suas ligações e outras ações similares, mas eles requerem um gigantesco conhecimento técnico, bem como uma torre falsa de recepção de sinal, e são tão raros e incomuns que não é necessário se preocupar com eles.

3.Como alguém pega um vírus no celular e como evitá-los?

Como já mencionamos, o primeiro passo é baixar um aplicativo ou abrir um arquivo desconhecido. É sempre importante ler as resenhas na loja antes de se comprometer com o download. Se você estiver em dúvida por causa de comentários controversos, não hesite em usar o Google e pesquisar um pouco a respeito do programa. Se não aparecer nenhum comentário particularmente negativo a respeito dele, sinta-se livre para baixá-lo. Outra atitude importante para evitar dores de cabeça é verificar as permissões que os aplicativos lhe pedem quando baixados. Afinal, por que um wallpaper precisa conhecer sua lista de contatos? Sempre desconfie de apps que requerem coisas que não estão ligadas às funções que ele descreveu na loja. A realidade é que a melhor forma de se proteger de malwares é sendo inteligente. Se você não instalar softwares crackeados e não oficiais, ou prestar atenção em tudo que você baixa, certamente não ocorrerá nada com o seu celular, e isso vale para qualquer sistema operacional.

4.Cuidado na hora de navegar

A internet das redes sociais é um prato cheio para URLs curtos que levam a sites mal-intencionados, spam, conteúdos duvidosos e até downloads de vírus. Desta maneira, assim como no seu computador, é importante tomar cuidado com os sites que você entra e especialmente com os links que você recebe. A dica mais vital é: nunca aceite a instalação de executáveis e outros arquivos quando estiver em sites com que você não está familiarizado. Ainda que seja incomum que você pegue vírus para celular desta maneira, ela pode ocorrer também.

5.Androids são mais inseguros que iPhones

Apesar do que alguns dizem, o Android é uma das plataformas menos suscetíveis a vírus. Estima-se que menos de 0.001% das instalações de aplicativos são capazes de trespassar a segurança da Google. Os poucos aplicativos maldosos que passam pelo crivo da empresa precisam romper uma série de barreiras até causar mal ao seu sistema. Primeiramente, o Android não lhe deixa instalar aplicativos dos quais não se sabe a procedência, uma opção previamente marcada e que impede a entrada de qualquer software maldoso no seu sistema. Se você ultrapassar esta segurança, ainda existem mais outras cinco precauções até ele ter acesso ao seu OS, como a verificação das permissões, a checagem de segurança de runtime etc. Esta fama de inseguro do Android se dá por sua liberdade. Qualquer um pode colocar um App na Playstore, enquanto a App Store deixa este privilégio reservado apenas para a própria Apple, que avalia caso por caso antes que alguma coisa entre. Apesar disso, existe uma ideia extremamente errada de que o iPhone é imune a vírus e malwares. Apesar do controle sobre os aplicativos, frequentemente descobrimos falhas de segurança no sistema operacional da Apple. A Symantec, uma das maiores empresas de segurança na web, escreveu um relatório reportando que encontrou cerca de 387 falhas de segurança no iOS; para o Android, o número de erros que eles encontraram foi de apenas 13. Outros métodos, como o Jailbreaking, que libertam o iPhone do monopólio da Apple, permitindo o acesso a outras lojas, o tornam ainda mais vulnerável do que o Android a aplicativos maldosos. Estima-se só na primeira semana do Evasion (programa de jailbreak) que mais de 7 milhões de usuários tenham feito uso dele, mostrando a força deste tipo de recurso na plataforma da Apple.

6.O vírus de celular pode se espalhar pelo ar

A não ser que falemos sobre redes de WiFi compartilhadas, ou que é possível baixar malwares a partir da sua conexão 3G, é praticamente impossível pegar um vírus pelo ar. A única possibilidade, como já mencionamos, seria se alguém montasse uma antena pirata e soubesse passar todos os firmwares de seu sistema. Ainda que casos como esse tenham aparecido nos Estado Unidos, eles são tão raros que nem entram em estatísticas.

7. Um vírus pode estragar ou queimar o celular?

A priori, um vírus de software nunca vai afetar o hardware do seu celular. No entanto, em raras ocasiões, ele pode danificar permanentemente o seu sistema, transformando o seu aparelho em um peso de papel elegante. Apesar disso, estes casos são extremamente raros e a maioria dos vírus hoje em dia deseja roubar informação ou replicar uma ação lucrativa para o hacker. Ninguém ganha nada simplesmente destruindo o sistema de um celular, por isso esse tipo de vírus é extremamente incomum.

8. Um vírus pode fazer seu celular drenar a bateria?

Certamente a presença de um vírus poderá afetar drasticamente a bateria do seu celular. Isso ocorre por que ele precisa utilizar sua memória e o seu processador para funcionar, efetivamente agindo como qualquer outro processo dentro do seu celular. Quanto mais processos você tem abertos, mais bateria você gasta, e, quanto mais eles exigirem de você, mais rápido sua bateria será drenada. Por essa razão, é possível dizer que isto não é um mito, ainda que não necessariamente um vírus vá gastar muito mais da sua bateria do que normalmente já é utilizado.

9. A maioria dos antivírus não funciona

Infelizmente esta informação não se trata de um mito. Todo este medo em torno dos vírus para celular criou um mercado muito grande para empresas dispostas a vender softwares prometendo proteção fácil para seus clientes. Um antivírus de verdade não pode ser produzido para os atuais sistemas operacionais dado os SDK (software development kits) e tipos de permissão e acesso para as empresas desenvolvedoras. Para detectar e acabar com vírus reais, um software precisaria ser rodado como um processo root no sistema, algo que simplesmente não é possível no Android e no iOS. No máximo estes programas funcionam como verificadores de assinatura, que monitoram os pacotes instalados de maneira atenta para qualquer erro de código ou linha suspeita. Mesmo empresas tradicionais, como a Norton, sofrem com “antivírus” que instalam dezenas de apps desnecessários e que não ajudam muito, por isso na maioria das vezes é melhor evitar a instalação deste tipo de aplicativo.

10. Alguns apps de defesa realmente ajudam

Nem todas as empresas são mal-intencionadas neste campo da segurança de celulares. Alguns aplicativos leves e gratuitos, como o 360 Mobile Security e o Avast, se focam naquilo que é mais importante: buscar códigos maliciosos, ficar atento a brechas no sistema operacional e, o mais importante, fazer com que o seu celular funcione de forma mais otimizada. Estes softwares vão escanear aplicativos antes de você baixá-los, vão verificar os diferentes URLs acessados pelo seu browser e no geral funcionam como um muro preventivo para que seu sistema não seja atacado. Na hora de escolher um bom software de proteção, faça o mesmo que recomendamos quando você tiver interesse por um app suspeito e pesquise intensamente sobre ele. Leia as resenhas na loja, depois vá ao Google e veja opiniões mais completas dos diferentes usuários.