ESCOLA DO CONSUMO
by Proteste

CURSO TECNOLOGIA NA PALMA DA MÃO - 60+

MÓDULO 2 - ESCOLA DE CONSUMO

Bem-vindos à Escola do Consumo!

A PROTESTE preparou cursos exclusivos e gratuitos destinados a todos os consumidores que querem se tornar mais conscientes em suas práticas diárias. O curso Finanças Domésticas Organizadas é o primeiro passo para que você organize o orçamento familiar, evite ficar no vermelho e tenha condições de planejar e realizar desejos e investimentos. Esta apostila, complementará as aulas ministradas por vídeo. Ela está dividida em três capítulos: Do mercado à Casa, Cuidados na Manipulação dos alimentos e Aproveitamento Integral dos Alimentos. Boa leitura e boas aulas.

Sobre a PROTESTE

Somos a maior associação de consumidores da América Latina, uma organização do Grupo Euroconsumers, líder global em informações inovadoras, serviços especializados e defesa dos direitos dos consumidores. Apoiamos os brasileiros em suas escolhas diárias de compras e contratação de serviços, seja por meio de nossos testes comparativos e estudos de mercado; seja por meio de eventos e debates de alto nível, com a participação de reguladores, instituições acadêmicas, empresas e organizações da sociedade civil; ou por meio de nosso serviço de defesa do consumidor, que pode ser acessado diretamente pela plataforma Reclame (www.proteste.org.br/reclame). Visite também o nosso site e saiba como se associar à Proteste.

www.proteste.org.br.

ESCOLA DO CONSUMO
by Proteste

Índice

Introdução

Smartphone é algo essencial na vida das pessoas na atualidade. Embora não tivesse esse termo, o primeiro aparelho celular que incluía múltiplas funções foi criado em 1992 pelo americano Frank Canova para a IBM (International Business Machines Corporation). Além de fazer o básico de um celular, ele ainda mandava e-mails, tinha calendário, calculadora e bloco de notas. Hoje em dia, o smartphone faz muito mais ações do que somente essas listadas, e aí que vem a complexidade de seu uso.

Antigamente era normal enfrentar filas no banco, ter a preocupação de não esquecer a habilitação ou o cartão do banco ao sair, utilizar um mp3 player para fazer exercícios, utilizar um aparelho de GPS (Sistema de posicionamento global) no carro, pedir comida ligando e ter uma maquina fotográfica para tirar fotos. Hoje essa realidade está diferente e ainda vai mudar bastante ao longo do tempo.

O smartphone virou um computador de bolso, até mais do que isso, um assistente para a vida do seu usuário, e agora será possível entender um pouco mais sobre o que ele tem para oferecer e os cuidados com o mundo digital.

Com a conclusão do curso, o aluno será capaz de conhecer melhor as redes sociais do momento, e poderá se comunicar por chats e videoconferência nos aparelhos celulares. Irá acessar fontes confiáveis de notícias e entender melhor o que é o termo “Fake News”. Além de saber como achar cursos online e escolher as melhores opções para atender a sua necessidade. O aluno também saberá como manter sua privacidade e segurança quando utilizar esse dispositivo, aprendendo como se proteger e manusear seus dados.

1. Melhore a comunicação

Antigamente o celular era feito somente para ligações, com o tempo o SMS e o MMS foram incluídos nas suas funções. Hoje, os métodos e modos para se comunicar são incontáveis. Até mesmo uma ligação pode ser feita de diversas formas. Aqui, nesse módulo, falaremos sobre as redes sociais, os mensageiros e as videoconferências.

POR DENTRO DAS REDES SOCIAIS

No Brasil, a primeira rede social que fez um grande sucesso foi o Orkut, e se manteve assim até que em 2011, quando ela foi ultrapassada em quantidade de usuários pelo Facebook. Nessa mesma época, a rede possuía 34,4 milhões de brasileiros ativos. Hoje em dia, temos diversas redes sociais sendo utilizadas, algumas mais famosas como o Instagram, o Facebook, o TikTok e o Twitter, e outras que são mais dedicadas a públicos e a temas específicos como o Clubhouse, Pinterest, Tumblr e o LinkedIn.
As redes sociais são espaços virtuais onde um grupo de pessoas se relacionam com outros usuários ou empresas compartilhando conteúdos como áudio, foto, vídeo ou mensagem. As redes sociais se diferenciam pelas suas funções principais, que podem ser dos mais diversos como jogar, divulgar produtos / serviços para compra e venda, compartilhar fotos e vídeos ou informações sobre temas variados, realizar networking ou estabelecer contatos pessoais.

Segundo o site Statista.com, a maior rede atualmente é o Facebook sendo seguido de perto pelo Instagram, porém existem diversas outras, vamos comentar sobre as mais famosas:

Facebook: praticamente impossível não começar pela principal e maior rede, atualmente, no Brasil. Com o maior número usuários, a chance de muitos amigos já terem acesso à rede, é muito grande. O Facebook promove interação com pessoas por meios de rede de amizades, compra e venda de produtos, grupos temáticos e jogos. Ao ingressar no Facebook será necessário informar o seu primeiro nome, o sobrenome, um numero de celular ou e-mail, uma senha, seu gênero e sua data de nascimento. Após isso já poderá adicionar seus amigos e postar frases, vídeos e fotos. É possível acessar o Facebook via aplicativo ou site.

Instagram: a mais popular entre os influenciadores. Cada dia que passa, mais o Instagram se destaca. Essa rede é mais baseada em fotos e vídeos. Enquanto o perfil do usuário do Facebook tem informações mais gerais, frases, pensamentos e argumentações dos usuários, o Instagram é voltada praticamente para imagens. Para ingressar no Instagram é preciso informar um número de celular ou e-mail, o seu nome todo, um nome de usuário, que não esteja sendo utilizado por outra pessoa, e criar uma senha. A interação é imediata, e com registro dos dados já é possível adicionar amigos a sua rede e enviar fotos para compor o seu perfil.

TikTok: Febre mundial em 2020/2021, a rede social chinesa atingiu o mundo com muita força na pandemia. Utilizada prioritariamente por pessoas de 16 a 24 anos, a rede é baseada unicamente em vídeos de curta duração. Aqui no Brasil, seu catalogo de vídeos postados são mais voltados para o humor, em sua grande maioria. Porém, informações e dicas também existem nessa rede.

Twitter: Nasceu em março de 2006, na época em que as redes sociais ainda não eram um foco para os usuários. Mas, com o tempo, o serviço explodiu em popularidade, e é uma das maiores redes até hoje. Ela serve como um blog em que as pessoas escrevem e comentam posts de conhecidos e desconhecidos. A informação costuma ser muito ágil, e os usuários ficam informados dos acontecimentos de forma muito rápida. Os assuntos são diversos, desde futebol à algum reality famoso, como informações de política, celebridades e até memes. Para criar uma conta é necessário um nome, celular ou e-mail e a data de nascimento.

Existem também as redes de relacionamento que são bastante utilizadas hoje em dia para conhecer pares amorosos. Existem diversas delas, mas o app mais conhecido é o Tinder. Nele o usuário cria um perfil com foto e biografia com visiilidade para os que navegam na rede. O acesso permite que o usuário escolha os perfis de seu interesse que aparecerem na tela, clicando no sim ou não. Caso os dois usuários tenham dado sim um para o outro, acontece o "match", e eles começam a conversar. Existem também outros apps de relacionamento que funcionam de forma parecida como o Happn e o Facebook Dating.

O importante na utilização de qualquer rede sociais é a segurança. Muitas delas causam exposição de dados como localização, imagens da casa do usuário e da maioria dos lugares em que ele vai, informações sobre os contatos mais próximos desse usuário, informações da biografia como

número de celular, e-mail, idade, estado civil entre outras diversas informações. É sempre importante se manter seguro nas redes sociais -, iremos abordar mais sobre isso no **Capítulo 3 - Segurança.**

Por se tratar de um universo novo, a linguagem acaba sendo diversificada. Nessas redes são usados muitos termos que podem ser difíceis de entender, por isso separamos alguns dos mais utilizados para poder explicar para vocês:

- #TBT: Throwback Thursday, usado quando é utilizada uma foto antiga na quinta feira.
- #PAS: Vem da palavra "Paz", existe um meme em que uma pessoa escreveu errado e isso viralizou.
- LOL: Usando quando a pessoa riu bastante. Vem do "Laugh out loud", que seria um "rindo muito alto".
- RT: É o Retweet, usado quando um usuário deseja compartilhar em sua rede alguma mensagem interessante publicada por outra conta.
- Direct ou DM: Significa enviar mensagem direta via o Messenger do Instagram.
- Stalkear: Procurar informações na internet e nas redes socais sobre um indivíduo. Para isso, o stalker (que vem da

palavra “perseguidor”) pesquisa atividades na internet sobre alguem ou as pessoas ao seu redor.

- Link na Bio: O link para a matéria ou conteúdo está na biografia da pessoa. A biografia, no Instagram, fica na pagina principal do perfil do usuário logo abaixo a foto do perfil.
- Feed: É o lugar onde fica o fluxo de conteúdo postado pelo usuário.
- DIX: Tipo de conta aberta somente para amigos íntimos.

VAMOS CONVERSAR SOBRE CHATS

Os celulares em 1992 ganharam o recurso de mensagem chamado SMS, desde lá e com a chegada dos planos pré-pagos o publico jovem começou a entrar no universo dos celulares. Os chats começaram a se popularizar no computador com o antigo ICQ e o Windows live Messenger, depois disso, cada vez mais chats foram incorporados por outras empresas e até mesmo redes sociais começaram a ter os seus próprios chats.

Os chats são programas ou aplicativos em que usuários conversam um com o outro via mensagens. Hoje em dia, os chats fazem parte da nossa vida e o mais conhecido deles é o Whatsapp. Ele é muito utilizado por pessoas, e até mesmo empresas integraram o sistema de comunicação com o cliente via Whatsapp. A maioria dos brasileiros possuem uma conta nesse aplicativo de mensagens, e isso fez dele o mais conhecido de todos por aqui. A maioria deles é gratuito, consumindo somente os dados de internet do pacote do usuário para funcionar. Seu consumo para mensagens é extremamente baixo, aumentando somente se for enviado arquivos, chamadas de voz ou chamadas de vídeo.

Para se organizar e controlar os gastos do dia a dia, alguns aplicativos permitem anotação o orçamento diário, semanal, quinzenal e mensal. Esses aplicativos são interativos, propõem desafios de gastos semanais, nos avisam quando ultrapassamos a média dos gastos com determinada conta, mostram possibilidades de renda extra, dicas de supermercados, informações sobre a economia em geral. O Olivia é uma desses aplicativos.

Além do Whatsapp, existem outros apps que também são famosos como o Telegram, o Facebook Messenger e o Direct Messenger (Instagram). Mas a lista disponíveis no mercado é enorme.

O Facebook Messenger e o Instagram Direct Messenger são os mensageiros das redes sociais. Embora muitos brasileiros tenham esses mensageiros, o Whatsapp ainda é o mais utilizado. Os dois são limitados na sua usabilidade, porém são atualizados constantemente. Para obter o Facebook Messenger é só fazer uma conta no Facebook, esse mensageiro possui seu aplicativo próprio chamado “Messenger”. Para obter o Instagram Direct Messenger é só fazer uma conta no Instagram. Esse mensageiro não possui aplicativo próprio. Vale lembrar que agora os dois mensageiros se unificaram, e é possível achar usuários do Facebook no Instagram, e vice-versa.

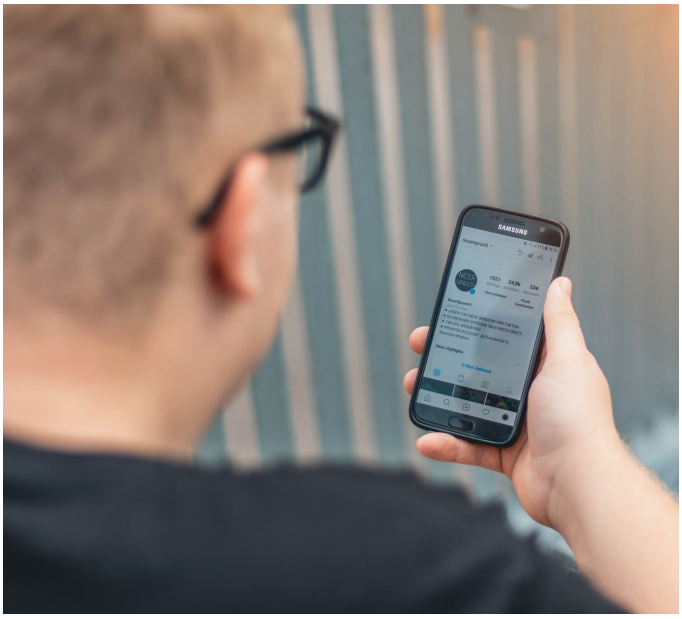
Caso o consumidor ainda não tenha uma conta no Whatsapp e queira criar, ele precisa do nome do usuário e do numero telefone para o processo. O aplicativo é gratuito, assim como as redes sociais; e utiliza a rede móvel ou Wi-fi para funcionar. É possível também fazer envio de documentos, vídeos, fotos e mensagens de voz. O usuário também pode acessar o mensageiro pelo computador, utilizando o Whatsapp Web, que é um clone do Whatsapp na tela do PC. Para acessar é só ir no endereço web.whatsapp.com, e ler o QRCODE com o whatsapp do celular. Para achar, é só ir em configurações e depois em **Whatsapp Web.**

O Telegram é um outro app de conversas que também é bastante conhecido e utilizado no Brasil. Mas tem algumas diferenças do Whatsapp que podem ser pontos negativos ou positivos para cada usuário. A primeira é que o histórico fica no servidor deles e não no smartphone. Então se o usuário acessar em outro aparelho, ele poderá acessar o histórico completo das conversas. Outra diferença é a quantidade de pessoas existentes em um grupo, que é

bastante limitado no Whatsapp, no Telegram são organizados supergrupos de até 200 mil usuários. Os canais do Telegram não têm limite de número de inscritos. Muitas empresas possuem supergrupos e canais para passar suas informações, principalmente notícias e discussão sobre temas específicos.

Atualmente o SMS e o iMessenger (mensageiro do iPhone) são muito utilizados nos Estados Unidos e em outros países. No Brasil é difícil ver pessoas utilizando tanto o SMS quanto o iMessenger.

Para finalizar esse tópico é importante falar sobre os atuais chatbots. Os chatbots são softwares que simulam a fala humana e são capazes de bater papo com usuários em um mensageiro. Ele é uma inteligência artificial preparada para responder perguntas direcionadas com a intenção de ajudar o usuário do serviço. Muitas empresas estão adotando essa ferramenta com o objetivo de conseguir auxiliar o consumidor sem precisar de interação humana. Atualmente, temos diversas chatbots no mercado, desde os mais simples que servem somente para iniciar o atendimento, quanto mais robustos que conseguem resolver problemas mais complexos.



VÍDEO CONFERÊNCIA EM PAUTA

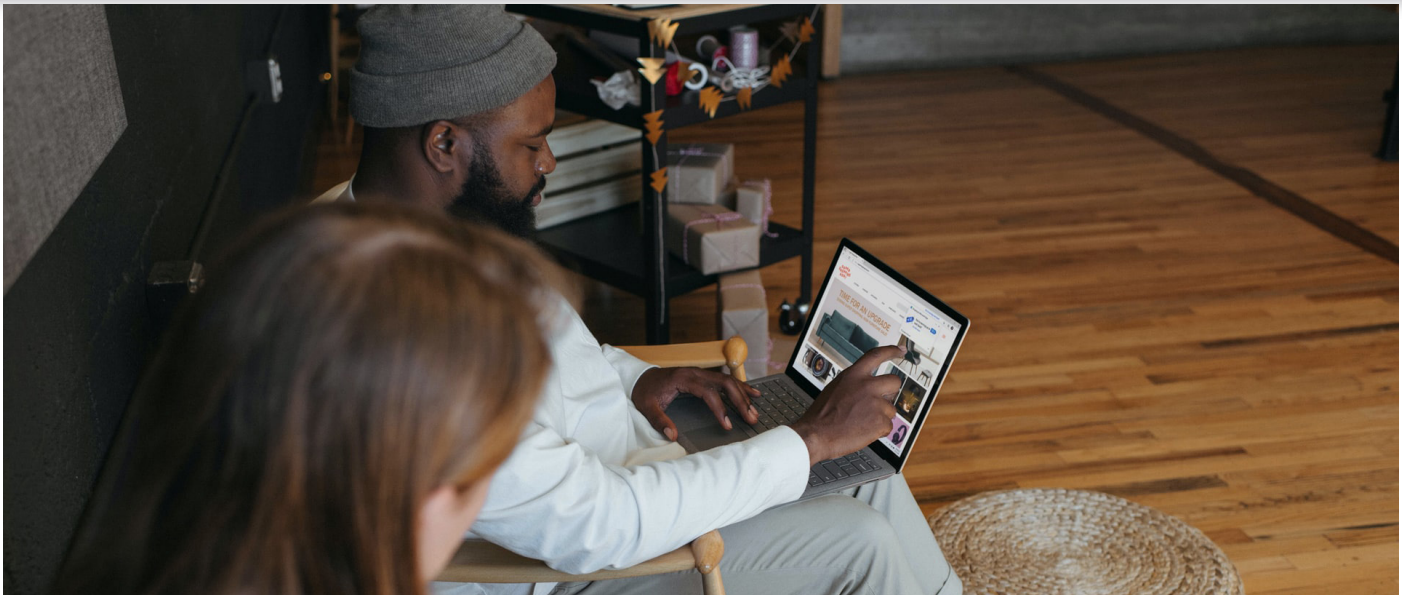
Com a melhoria da conexão, a chamada de vídeo começou a ser mais utilizada pelos usuários. Embora consuma muito mais do que as mensagens escritas, a vídeo chamada se tornou mais relevante e acessível com a consolidação da tecnologia 4G.

Hoje, no mercado, a maioria dos mensageiros já possuem chamadas de vídeo, como o Whatsapp, Instagram Direct Messenger, Telegram e o Facebook Messenger. Porém existem aplicativos mais voltados para o uso como o Google Duo, presente tanto no Android quanto no iOS, o Facetime que é só para iOS e o Skype que é mais conhecido por chamadas de voz, mas também possui a função vídeo e escrita, presentes nas lojas de apps. Contudo, esses são apenas alguns apps de videoconferência disponíveis.

Existem alguns aplicativos de vídeo chamada mais voltados para grupos específicos, como o Zoom e o Microsoft Teams, que são mais usados para empresas, Discord que é mais usado por games e grupos de pesquisa, e o Houseparty que é mais usado para festas e aniversários. Para se cadastrar em qualquer um deles é só baixar o app oficial. A diferença desses aplicativos, mais específicos para empresas, é que eles conseguem colocar na mesma conferencia uma quantidade muito maior do que os mensageiros convencionais. Para ter uma ideia, o Whatsapp consegue até 8 pessoas em uma vídeo chamada enquanto o zoom permite 1000 participantes com vídeo e o Microsoft Teams conecta 100 pessoas ao mesmo tempo por vídeo.

Para empresas existem algumas outras funções importantes nesses aplicativos de vídeo chamada como o compartilhamento de tela e controle de tela, que funcionam somente nos computadores, e a função apresentação, em que um usuário pode mostrar um documento para todos do grupo.

2. Conhecimento e informação nunca são demais



O que antes era procurado em livros hoje em dia são mais procurados em livros digitais, cursos estão se tornando online, bibliotecas estão se adaptando, também, a espaços digitais, e, a cada dia que passa, mais a internet se consolida como a melhor e maior forma de busca por informações e conhecimento.

Segundo uma pesquisa do Statista, em 2019 tínhamos online mais de 1,7 bilhões de sites e é esperado que hoje em dia exista muito mais. Com todo esse conteúdo online, mais e mais pessoas se conectam na internet. Segundo a TIC Domicílios 2019, três em cada quatro brasileiros acessam a internet, o que equivale a 134 milhões de pessoas.

Um fluxo grande de pessoas produz muita informação na internet, e como muita gente tem acesso e muito conteúdo é gerado, acabam existindo informações mentirosas, duvidosas, equivocadas ou sem fundo científico para embasamento. Por isso, é muito importante saber onde procurar a informação certa e fidedigna nesse universo.

FILTRE O QUE TE INTERESSA

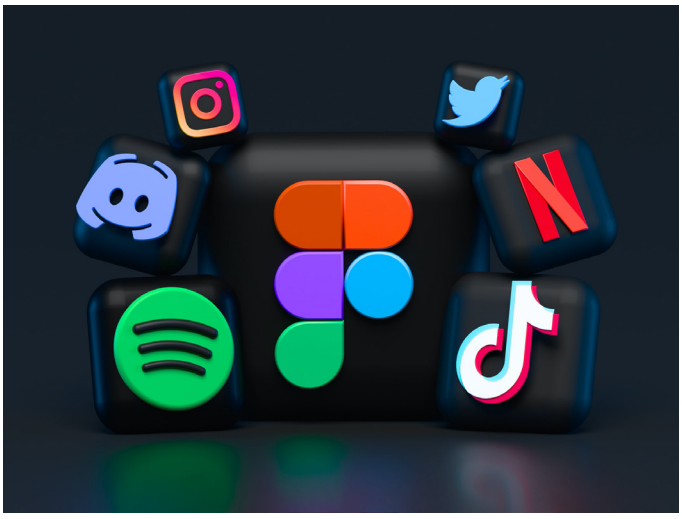
Nesse mar de informações existentes na internet, achar a que você procura pode ser difícil, e aí que surgiram os famosos buscadores. Os sites mais conhecidos da internet desde sua popularização. Os buscadores são websites especializados em buscar e listar páginas da internet a partir de palavras-chave que são indicadas pelo usuário. Hoje em dia, os buscadores são verdadeiros motores de procura, pois fazem uma enorme varredura de toda rede mundial rastreando essas palavras-chaves informadas.

Existem os buscadores globais, como o conhecido Google, além do Yahoo e o Bing da Microsoft, entre outros menos conhecidos. Porém, existem buscadores mais específicos ou regionalizados como o Catho e o Vagas.com para empregos, e o GuiaMais para pesquisa de DDD ou o TripAdvisor para conhecer estabelecimentos em viagens.

Ao realizar uma pesquisa em um buscador ele vai direcionar primeiro os sites com maior relevância, ou seja, que são bastante visitados e acessados de forma orgânica com conteúdo considerado relevante, além dos sites que pagaram por esse destaque. Normalmente os sites com bastante relevância possuem conteúdos com qualidade. Porém, existem métodos de conseguir filtrar melhor os termos buscados para que o conteúdo apareça com mais facilidade. Além de ser bem breve nos termos usados para serem buscados, deve-se evitar termos desnecessários pois irá confundir o buscador. Para facilitar a busca segue uma lista para uma busca facilitada no Google:

- **Pesquisa de frase específica:** se a busca for pelo tema desenvolvimento sustentável, o Google irá trazer informações tanto para o termo desenvolvimento quanto para o termo sustentável. Caso seja necessário os termos juntos, é só colocar entre aspas. Exemplo: “desenvolvimento sustentável”.
- **Excluir palavras:** se for necessário retirar algum termo na busca, é só informar a expressão ou palavra que deve ser retirada com um sinal de menos.
Exemplo: “Desenvolvimento sustentável” -economia.
- **Pesquisa por um ou mais termos:** se a procura for por um ou mais termos, é só digitar a palavra OU entre as palavras da busca.
Exemplo: Fertilizante **OU** Nitrato.
- **Palavras no texto:** se a procura for por palavras dentro de um texto. Inclua a comando **allintext**:, antes da busca. Dessa forma irá vir algum texto que tenha essas palavras nele.
Exemplo: **allintext:** Europa passagem valor hospedagem.
- **Palavras no texto e no título:** na busca por palavras que estão no texto e outra expressão que esteja no título. É só colocar o primeiro termo que vai informar o que você busca no texto e depois o comando **intext:** seguido com o segundo termo que pode estar no título ou na URL.
Exemplo: Marvel **intext:**Thanos.
- **Palavras no título:** se o objetivo for palavras que estão no título da notícia ou da matéria é só usar o comando allintitle:.
Exemplo: **allintitle:** Amor de mãe.
- **Pesquisa dentro de um site:** quando a pesqisa acontecer por algo específico dentro de um site, também, específico é só usar o comando site:.
Exemplo: site:proteste.com.br “Galaxy S21”.
- **Pesquisa relacionada:** serve para achar sites com conteúdo parecido com um outro site é só usar o comando related:.
Exemplo: **related:**globo.com.
- **Sinônimos ou palavras similares:** tem como objetivo incluir na busca uma palavra específica e também outra similar a ela, para isso é só usar o símbolo ~.
Exemplo: Gato ~Felino.
- **Definições de palavras:** tem como finalidade verificar o conceito da palavra ou frase, basta usar o comando define:.
Exemplo: **define:**protagonista.

Vale lembrar que os aplicativos dos principais buscadores estão disponíveis na AppStore e na PlayStore.



CUIDADO COM AS FAKE NEWS

Fake News é um dos termos mais conhecidos ultimamente, devido a pandemia e as eleições de 2018. O termo vem do inglês fake que quer dizer falso e do news que quer dizer notícia. Apesar de ter se destacado ultimamente, a expressão é antiga e data do final do século 19. Fake News são as informações falsas que viralizam entre a população como uma informação verdadeira por comunicação boca a boca, por meio digital, marketing ou por notícias. Atualmente essas Fake News se propagam mais fortemente pelas redes sociais e pelos mensageiros.

Desde a antiguidade, verdade e mentira se misturavam entre todas as informações passadas entre a população. As propagandas enganosas sobre remédios milagrosos foram uma das primeiras Fake News existentes, e desde lá cada vez mais notícias falsas aparecem.

Com a chegada da internet e com o aumento de usuários mais notícias se espalham, e com uma velocidade cada vez mais rápida. Uma Fake News viralizar não é muito difícil, e já tivemos diversos casos de fotos adulteradas, informações falsas sobre políticos nas eleições e até mesmos vídeos reais que são usados para ilustrar outros momentos que tiveram um contexto diferente.

Divulgar Fake News é uma pratica perigosa, compartilhar essas informações falsas como fotos e vídeos manipulados e publicações duvidosas pode trazer risco para a saúde pública, incentivar o preconceito, a violência e, até mesmo, resultar em mortes causadas por desinformações.

- Saúde pública: O grande motivo dos movimentos antivacinação cresceram muito nos últimos anos. As pessoas negacionistas acabam gerando notícias falsas e propagam sua visão de que a vacina faz mal para a população enquanto a ciência prova o contrário.
- Disseminação de violência: Posições divergentes tanto a uma ideologia política quanto a uma difamação direta para alguém pode acabar alimentando o discurso de ódio e, em consequência disso, a violência verbal e física.
- Transtornos para a população: Em 2018, existiu um medo de uma nova greve dos caminhoneiros, pois a gasolina ficou escassa no momento da greve. Por causa de uma Fake News, filas enormes de carros para abastecer acabou parando alguns municípios de forma desnecessária.
- Falsas acusações: Falsas acusações de pedofilia ou qualquer outro tipo de crime, sem ser investigado, acabou causando a morte de diversas pessoas no mundo todo.
- Influência política: No momento das eleições é possível identificar diversos tipos de Fake News que são produzidos para alimentar ódio aos candidatos e fazer a popularidade deles diminuirem.

Nesse mar de informações existentes na Internet é imprescindível que o usuário fique alerta para não disseminar nenhuma informação falsa em suas redes. Para isso, é sempre importante verificar a fonte da informação. Normalmente grandes sites de notícia como Globo.com, Folha de São Paulo, Extra, UOL, MSN, CNN, BBC entre outras empresas conhecidas no mercado se preocupam com a verdade. Além disso, é importante verificar sempre que tenha dúvida. Existem sites especializados em verificar notícias. Entre eles existem: o boatos.org, Aosfatos, UOL confere, Truco, E-farsas e Agência Lupa.

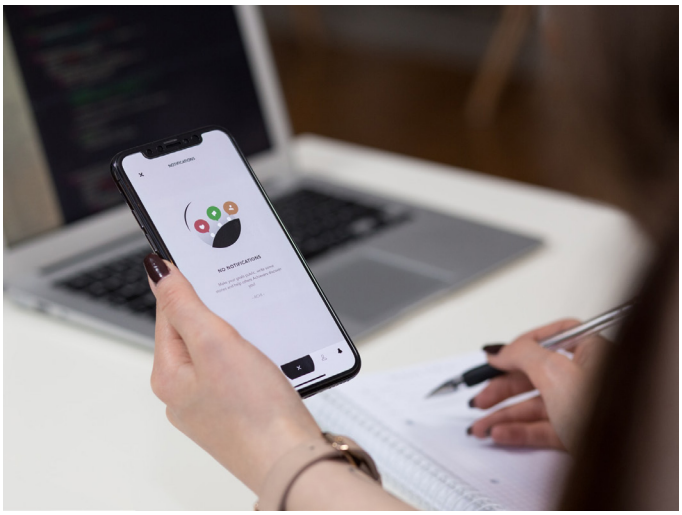
Para combater a Fake News, é necessário verificar as fontes e avisar aos seus amigos e amigas caso eles tenham compartilhado uma notícia falsa. Cada cidadão deve assumir o compromisso de verificar os fatos antes de compartilhá-los na rede, e até mesmo de acreditar em tudo que circula por lá.

COMO ESCOLHER CURSOS PELA INTERNET

Os cursos online são uma realidade e a cada dia que passa mais estão sendo procurados e consumidos. Depois do início da pandemia, especializações de EAD (Ensino a distância) tiveram um crescimento de 130%. A FGV, por exemplo, apresentou um crescimento de 400% na adesão das formações online gratuitas em comparações com os meses de janeiro e fevereiro de 2020, antes do início da pandemia, aqui no Brasil.

A educação a distância é reconhecida pelo Ministério da Educação como uma forma viável de adquirir conhecimento e, por isso, pode ser a melhor opção para pessoas que não possuem tempo para se locomover ou moram longe dos centros urbanos. Existem diversos benefícios nessa forma de ensino, como definir seu próprio horário, assistir a aula completa mais de uma vez, parando ou repetindo quantas vezes quiser, além das conversas por mensagem com os professores e outros alunos.

Hoje em dia, na internet existem diversas empresas oferecendo ensino a distância dos mais diversos tipos. Até mesmo agregadores de cursos estão disponíveis no mercado como o Alura e Udemy. Com esse mercado rico de formações e muitas metodologias diferentes para explicar diversos temas, fica difícil saber qual será a melhor para cada usuário. Sendo assim destacamos os pontos que cada aluno deve verificar antes de iniciar um curso online:



- O primeiro passo é saber qual empresa ou pessoa oferece o curso. É importante que o professor ou empresa seja capacitada para passar o conteúdo para o aluno de forma eficaz. Para isso o aluno pode procurar informações na internet sobre o ensino ou procurar os professores no LinkedIn para saber mais sobre a vida acadêmica e profissional deles.
- É importante que o curso tenha informações sobre o tempo necessário para o aprendizado, informações de quantidade de download necessário para completar o cronograma de aulas, quanto tempo o aluno terá acesso ao conteúdo, e onde ele estará disponível, e, ainda, se terá certificado ou não. É importante que a empresa emita um certificado de conclusão para que o aluno comprove o conhecimento adquirido.
- É obrigação do curso online informar os requisitos necessários para o início da formação. Alguns cursos precisam de certos programas que podem ser custosos e por isso devem ser descriminados antes.
- É obrigação do curso informar quais as experiências ou os entendimentos necessários para o início do curso. Assim como deixar claro qual será o conhecimento que o aluno terá após a conclusão.

Os usuários de curso online precisam tomar cuidado com influenciadores que não possuem conhecimento técnico para produzir conteúdo. Por exemplo, uma influenciadora que faz academia e está em forma com o corpo não pode falar sobre alimentação se não for nutricionista ou tenha algum curso especifico para essa área. Porém, ela pode fazer parte de um curso mostrando como a organização alimentar fez bem para a vida dela, em conjunto com especialistas na área.

3. Segurança

A segurança é o item mais necessário no ambiente online, já que a rede se torna cada vez mais perigosa com o passar do tempo. Os relatórios da AVTEST mostram que o crescimento de malware quase dobrou de 2015 para 2019, ou seja, a cada ano que passa mais software mal-intencionados estão circulando pela internet.

O malware é a abreviação de "software malicioso" e ele pode infectar computadores e dispositivos de diversas maneiras, além de assumir diversas formas. Seguem abaixo algumas das mais importantes delas:

- **Vírus:** Um vírus de computador é uma parte de um código malicioso que é pré-anexado ou anexado a arquivos existentes no computador. O nome vem dos vírus biológicos pois eles utilizam técnicas semelhantes para se espalhar de um lugar para o outro. O termo vírus é usado erroneamente para qualquer tipo de ameaça em um dispositivo. Para isso o termo mais correto seria malware. O vírus ataca principalmente os arquivos e documentos executáveis, ao clicar em um arquivo executável infectado, o vírus é ativado. Eles são perigosos pelo potencial em destruir arquivos do disco rígido.
- **Worm:** É um programa contendo código malicioso que ataca os computadores e se espalha na rede. A diferença entre o vírus e o worm é que o worm tem capacidade de se espalhar por conta própria. Os worms propagam-se para os endereços de e-mail da lista de contatos ou aproveitam-se de vulnerabilidades da segurança dos aplicativos de rede. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware. Ele pode excluir arquivos, prejudicar o desempenho do sistema e até mesmo desativar programas. Ele é um meio de transporte para outras infiltrações.
- **Trojan:** Também conhecidos como "cavalo de tróia", eles tentam se apresentar como programas úteis, enganado assim os usuários que os executarem. Existe uma ampla subcategoria para eles, os downloader possuem a capacidade de fazer download de outras ameaças da internet, o dropper possuem a capacidade de instalar outros malwares, backdoor que se comunicam com atacantes remotos dando a esse o acesso ao computador e Keylogger que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- **Adware:** É abreviação de "advertising-supported software" ou software suportado por propaganda. São programas que exibem material de publicidade. Eles abrem automaticamente uma nova janela pop-up contendo publicidade da Internet no navegador ou mudam a página inicial do mesmo. O adware é frequentemente vinculado a programas gratuitos, permitindo que seus criadores cubram custos de desenvolvimento de seus aplicativos que são geralmente úteis. O Adware não é perigoso, porém alguns podem ter funções de rastreamento. Sempre ao instalar um programa ou app verifique se existe publicidade no mesmo.
- **Spyware:** Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento ou conhecimento do usuário. Os spyware usam funções do celular ou computador para enviar informações como sites visitados, endereços de e-mail da lista de contatos, números de telefone, lista de teclas registradas entre outras informações para servidores remotos. Muitos produtos e serviços gratuitos tem vinculado um spyware.
- **Ramsomware:** É um tipo de malware que bloqueia seu dispositivo ou criptografa o conteúdo no seu dispositivo e extorque dinheiro do usuário para restaurar o acesso ao conteúdo. Esse tipo de malware pode ter um timer embutido com um prazo para pagamento. Caso tenha contato com esse malware e tenha um arquivo pessoal travado entre em contato com a polícia.

Esses malware são criados por criminosos virtuais com o intuito de roubar os dados e prejudicar o computador ou dispositivo das pessoas. Para se proteger deles é possível instalar programas e apps chamados antivírus ou Internet Security criando barreiras de proteção no seu dispositivo. De qualquer forma, não existe proteção absoluta contra eles. A melhor defesa é a combinação de um bom uso da Internet e ferramentas bem desenvolvidas para garantir ao seu computador ou smartphone uma boa segurança.

Além do Malware existe o PUA que é o aplicativo potencialmente indesejado. Eles não têm um objetivo claramente nocivo quanto os outros tipos de malware, como vírus e cavalos de tróia, porém eles podem instalar um software indesejado adicional, alterando o comportamento do dispositivo digital ou realizando atividades não aprovadas ou esperadas pelos usuários. Esse aplicativo potencialmente indesejado pode ser um aplicativo que é um software legítimo, mas que também pode ser usado por uma pessoa indevida.

Quando o assunto é smartphone, não é fácil identificar se o aparelho está infectado, principalmente porque o software malicioso pode não estar visível. Por isso é importante fazer a reinstalação do software do seu dispositivo pelo menos uma vez ao ano, sempre após um backup dos dados que precisam ser salvos. Porém, alguns malwares acabam deixando alguns rastros como muitos anúncios ou solicitações de permissão, consumo de bateria em excesso e aplicativos desconhecidos instalados no celular. Em alguns casos o app desconhecido não apaga, nem mesmo forçando. Para solucionar todos esses casos, a melhor opção é a reconfiguração do sistema operacional do aparelho. Para isso, no iOS é só ir em ajustes, geral, redefinir, e depois em apagar conteúdo e ajustes. No Android, é precisa acessar as configurações, gerenciamento geral e restaurar, e depois em restaurar padrão de fábrica. Essa função apagará o malware e todos os seus arquivos, então é importante que o usuário salve o que for necessário. Tudo começa com a pergunta:

CUIDADO COM SEUS DADOS

O que são dados? Dado é o valor atribuído a alguma coisa ou pessoa. Ao ver uma foto de um objeto é possível identificar a cor, o tamanho, se é novo ou usado e o tipo de utilização. Esses são os dados.

Os dados do usuário são dados referentes a uma pessoa. Essas são as informações mais desejadas pelo marketing das empresas e, por isso, elas valem tanto. Empresas como o Google utilizam os dados dos seus usuários como principal fonte de renda no seu negócio. Quando é falado “dados do usuário” normalmente as pessoas pensam em e-mail, telefone e nome, mas eles vão muito além disso.

A coleta dos dados por parte das empresas é feita de diversas formas, de modo geral podemos chamar esses dados de sensíveis ou anonimizados. Os dados sensíveis são as informações particulares como e-mail, telefone e CPF ou até mesmo etnia, opinião política, convicção religiosa ou sexual. O anonimizado é o dado que não se identifica que o gerou, e não são considerados pessoais. Como exemplo temos o tempo que o usuário ficou em uma página, a velocidade da internet dele ao usar um velocímetro ou a pesquisa realizada em um site de buscas.

Hoje em dia, no Brasil, existe uma lei de proteção de dados chamada LGPD, a Lei Geral de Proteção de Dados, que passou a valer desde agosto de 2020. e visa proteger os consumidores. A Proteste atua fortemente nessa área oferecendo cursos e cartilhas para ajudar pequenas e médias empresas nessa tema.

A lei tem como foco o respeito a privacidade, direitos humanos e exercício da cidadania, desenvolvimento econômico e tecnológico, concorrência e livre iniciativa, controle sobre dados pessoais e o direito a intimidade, honra e a imagem. Com esses pilares, o consumidor se sentirá mais protegido e as empre-

sas saberão o que podem fazer com os dados de seus clientes.

De qualquer forma os dados pessoais devem estar sempre seguros para que ninguém sofra algum tipo de ataque virtual. Uma pessoa mal-intencionada, com o nome do usuário, CPF e numero de cartão de alguém pode realizar compras e gerar um grande problema. Qualquer dado sensível em mãos erradas podem ser um perigo, por isso é importante que o usuário fique em alerta ao entregar suas informações.

Existem certos passos que devem ser tomados sempre que estiver utilizando um serviço:

- Caso a empresa peça algum dado, o consumidor deve sempre perguntar qual será o uso daquele dado. Algumas empresas pedem muitas informações desnecessários, e que podem acabar vazando por uma falta de segurança, prejudicando o consumidor.
- Os aplicativos no celular informam quais funções e dados vão ser utilizados antes da instalação. É importante verificar se os dados são coerentes para o serviço prestado.
- Ao baixar aplicativos e programas, é sempre importante o usuário utilizar as lojas oficiais e confiáveis para realizar esse download. Lojas desconhecidas podem ter aplicativos fraudulentos.
- Para fazer compras ou cadastros, é importante que o consumidor tenha um e-mail somente para isso. A caixa pode acabar cheia de e-mails indesejados se ocorrer a venda dos dados para outra empresa.
- Cartão de crédito, nome completo, endereço, CPF e RG são dados muito sensíveis, e só devem ser digitados em sites ou apps de confiança.
- É importante verificar se o site acessado é seguro, procurando informações ou selos de segurança embutidos nele.
- No momento da finalização da compra, deve ser identificado qual empresa vai entregar e quem é o distribuidor.
- Posts nas redes sociais podem acabar dando dados sensíveis, e isso pode ser um grande problema. Ao tirar fotos de documentos, como a carteira de vacinação do Covid-19 ou uma chegada de um novo cartão de crédito, sempre oculte os dados que não são necessários na postagem.

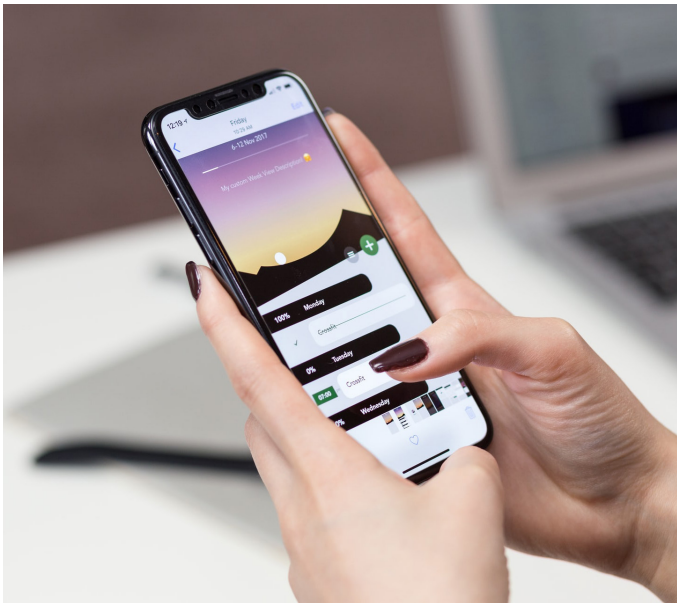
As redes sociais são um problema a parte quanto a privacidade e vazamento de dados. Como elas acabam dando a possibilidade de ser uma vitrine para os seus dados, é importante que o usuário peneire alguns. Sendo assim, quantos mais dados compartilhar na Internet, mais vulnerável ficará. A disseminação de conteúdos tem um alcance inimaginável. Por isso, faça uma gestão cuidadosa daquilo que realmente quer que os outros saibam de sua vida. É possível que você não queira que todo mundo possa ver suas fotos da festa de sábado. Para isso, você pode escolher o que compartilhar, com quem e de que forma. Porém, o mais importante a se perguntar é se é realmente necessário publicar.
Todas as redes sociais possuem controle de privacidade que podem ser achados na configuração de privacidade ou privacidade e segurança. Existe a possibilidade de manter o perfil fechado para pessoas que não estão adicionadas.

O navegador da internet também mantém os dados salvos, como histórico de pesquisas, cookies, cache, dados da navegação, informações até mesmo sobre login utilizado em um acesso ao e-mail. Por isso é importante sempre estar apagando os dados que podem ser achados em configuração e, depois, em privacidade e segurança. Caso esteja em um dispositivo desconhecido é melhor utilizar a aba de navegação anônima.

Os buscadores também salvam o histórico caso estejam logados, então para que não salve o histórico é só deslogar. Ao buscar alguma informação nos buscadores sobre você e os resultados forem inadequados, irrelevantes ou excessivos, é possível solicitar a retirada judicialmente.

Caso o usuário seja vítima de um ciberataque e tenha seus dados roubados ou sequestrados, ele deve reportar imediatamente a delegacia de crimes virtuais. Caso não haja delegacia especifica para crimes virtuais na região, a polícia normal deverá ser informada sobre o crime. Caso o usuário acredite ter sido vítima, é importante que ele pegue o maior número possível de provas para evidenciar o caso, tirando print da tela, anotando informações, como data e hora do acontecimento ou quando descobriu o furto.
Em alguns casos, empresas podem ser hackeadas e vazarem os dados dos usuários. Sempre que forem noticiados esses casos, o usuário deve entrar na sua conta e mudar a senha imediatamente. Caso seja possível a ativação da senha em duas etapas é importante que ative.
Vale lembrar que os dados dos usuários podem ser roubados ou furtados fisicamente também, como no roubo ou furto de um smartphone. Para evitar o vazamento de dados nesses casos, mantenha sempre uma senha segura na tela de bloqueio do celular, como uma senha biométrica ou com letras e números. Além disso, é importante colocar a senha chamada PIN do CHIP/SIM. Essa mudança pode ser feita nas configurações do aparelho em rede ou celular. Dessa forma, ao reiniciar seu aparelho será pedido a senha do chip.

O QUE OBSERVAR NA HORA DAS COMPRAS ONLINE



As compras online estão em amplo crescimento nos últimos tempos, principalmente depois do inicio da pandemia em 2020. Segundo dados da IPSOS, 47% dos habitantes do Brasil tem feito mais compras online do que faziam antes da COVID-19. E isso não é só no Brasil, mas no mundo todo.
Com esse crescimento, mais lojas online aparecem no mercado. Segundo o Paypal, o número de lojas cresceu 40,7% de agosto de 2019 até agosto de 2020. Com o crescimento do mercado, mais crimes cibernéticos acontecem e por isso todos os consumidores devem ficar em alerta.

Para o consumidor realizar uma compra segura ele deve prestar bastante atenção em alguns pontos que listamos abaixo:

- É interessante que o consumidor prefira lojas conhecidas no mercado. Caso opte por uma loja desconhecida, ele deve procurar na internet por outras pessoas que utilizaram a mesma loja para ter certeza da integridade.
- Deve ser evitado clicar em links de e-mail ou marketing que direcione para a loja virtual. Sempre prefira entrar na loja e procurar o produto desejado.
- Alguns sites usam selos de confiança e eles devem ser verificados. Para fazer isso é só clicar no selo e verificar se a empresa está mesmo certificando a loja virtual.
- A barra de pesquisa deve estar em HTTPS pois dados sensíveis serão utilizados como o número do cartão. Para saber se o site é HTTPS é só verificar o início do link da página ou procurar por um cadeado na esquerda da barra de pesquisa do navegador.
- Existem muitos casos de sites que são copias das lojas virtuais conhecidas que se passam por elas para pegar dados dos consumidores. Para saber se a loja é a correta, é só olhar o link da barra de pesquisa do navegador. Ela deve iniciar exatamente como a loja virtual e não com nomes “saldao” ou “promocao” no link.
- Existem sites de reclamação em que consumidores falam sobre sua experiencia na compra, é fundamental usá-lo para saber

como uma loja se comporta nos momentos de entrega e pós-venda.

- Toda loja virtual tem que ter a política de troca e devolução de maneira acessível. É necessário verificar se a empresa possui essas informações.
- É importante observar se o site tem fácil acesso ao SAC caso seja necessário fazer uma reclamação da compra.

Um dos maiores motivadores de compra são os reviews de influenciadores e outros usuários que adquiriram o produto desejado. Eles devem ser levados em conta para o momento da compra. É importante saber como o produto se comportou na sua utilização, pequenos problemas de usabilidade são facilmente achados nesses reviews de usuários e por isso eles são importantes, porém, existem casos que devem ser ponderados. Embora todas as grandes empresas de comercio eletrônico combatam esse tipo de problema, o fake reviews existe e deve ser evitado.

Na medida em que fóruns, blogs ou sites com rankings de produtos a partir de avaliações se tornam mais importantes (tendo mais visibilidade), suas opiniões ficam na mira de empresas que querem ter as melhores avaliações possíveis para aumentar suas vendas. E, para ter as melhores opiniões em combinação com a ausência total ou parcial de controles que garantam a confiabilidade delas, algumas revisões podem ser falsas e dai que vem o termo variando do fake news, o fake reviews.

Um review falso normalmente é positivo (geralmente de 5 estrelas), e é deixado em um produto por alguém que pode nem ter sido o comprador e agir em nome do vendedor. Em alguns casos é isso - o próprio vendedor com um nome de usuário diferente. Fake reviews geram péssimas experiências, pois mostram uma imagem enganosa do produto e incentivam à compra de algo que pode estar abaixo do padrão divulgado, basicamente, usando uma publicidade falsa. Existem casos em que as avaliações são alteradas após intervenções do vendedor, como, por exemplo, quando a loja oferece algum tipo de benefício após a postagem do comentário. Assim, ele pode acabar dando um tratamento diferente somente aos consumidores que procuram pelos seus direitos, dando a falsa sensação de que está tudo bem com as diversas boas avaliações das pessoas cujos problemas foram sanados.

A consultoria inglesa BrightLocal identificou que 79% dos consumidores online tiveram contato com avaliações falsas em 2017, mas 84% destes não saberiam como identificá-la. Estima-se que 20% de todas as avaliações sejam falsas, e os especialistas da FGV dizem que isso se aplica, também, ao Brasil.

Segundo o site AMZdiscover, em 2012, o escritor criminal RJ Ellory foi suspenso da Amazon quando foi descoberto que ele havia deixado uma crítica falsa para um de seus romances, chamando-a de ‘obra-prima moderna’, além de deixar críticas negativas para autores concorrentes. Este é um exemplo clássico de por que alguém publicaria uma crítica falsa.

Há várias razões pelas quais as pessoas deixam críticas falsas para produtos em lojas virtuais, mas, em suma, o principal motivo é vender mais um produto. As principais razões para deixar comentários falsos são:

- Melhorar a classificação do produto.
- Melhorar a classificação do vendedor.
- Aumentar as vendas de produtos com baixa venda.
- Aumentar a visibilidade dos produtos que acabaram de ser listados.
- Equilibrar as críticas negativas para um produto.

Existem três modelos de avaliação:

- Espontânea: o cliente revisa sua própria opinião sobre o produto ou serviço, sem nenhum tipo de estímulo.
- Estimulada: a empresa oferece dinheiro ou benefício em troca de avaliação positiva para si própria ou negativa para o concorrente.

• Comprada: usuários pagos para avaliar sem, necessariamente, ter consumido o produto ou serviço.

Ao deixar uma avaliação extremamente positiva de um produto, a classificação do ítem aumenta, e, consequentemente, eleva a sua visibilidade. Espera-se também que os clientes em potencial leiam essas análises, e comprem o produto por influência delas.
Em casos extremos, comentários falsos podem ser deixados para produtos que nem existem, mas que foram listados por um vendedor como um ato de fraude.
Os revisores falsos são capturados e suspensos pelas lojas virtuais sempre que possível, mas há alguns pontos que podem ser observados para conseguir identificar se a avaliação do produto é potencialmente falsa:

• Muitas críticas positivas foram deixadas em um curto espaço de tempo, geralmente usando palavras e frases semelhantes.
• Muitas críticas com fotografias idênticas ou muito semelhantes (o melhor é verificar o plano de fundo quanto a roupas ou ambientes não muito formais)
• Comparação negativa do produto de um concorrente, do tipo: “prefiro esse do que o outro” principalmente, sendo produtos caros, que, dificilmente, o usuário teria chance de comprar os dois.
• Muitas resenhas de 5 estrelas com conteúdo muito curto - geralmente quando alguém fica encantado o suficiente para deixar uma resenha com esta pontuação, fica muito disposto a escrever algo sobre o produto.
• As críticas são positivas, mas sem detalhes sobre os recursos, a facilidade de uso, etc.
• Uso persistente do nome completo do produto.
• Uso estranho de linguagem que pode significar uma tentativa de usar palavras-chave para fins de SEO (facilidade de ser buscado pelo Google).
• Revisões que elogiam demais o produto, principalmente algo que dificilmente seria elogiado.
• A resenha é deixada por alguém que deixa constantemente apenas avaliações de 5 estrelas.
• Uma crítica positiva postada no dia da listagem do produto ou logo depois.
• Comentários que não estão anexados a uma compra “verificada”, o que significa que o revisor pode nem ter comprado o produto.
• Várias revisões usando linguagem semelhante e listando os mesmos benefícios.
• Pouco ou nenhum histórico de classificação do revisor - isso pode significar que a conta do usuário foi aberta com o único objetivo de deixar comentários para os produtos desse vendedor.

Nos Estados Unidos e na Europa existem ferramentas online que conseguem identificar se o Review é potencialmente falso, porém no Brasil não conseguimos encontrar algo semelhante. Atualmente, só possuímos ferramentas para fake news enquanto os fake reviews continuam desamparados.

COMO UTILIZAR APLICATIVOS DE FORMA SEGURA

O Brasil é o 3° país em que pessoas passam mais tempo em aplicativos. Em média, as pessoas passam entre 3 horas e 40 minutos por dia usando aplicativos, segundo as informações divulgadas pelo App Annie sobre os dados de 2019. O país só é superado pela China e pela Indonésia. Por isso que várias empresas estão criando bastante aplicativos com intuito de manter cada vez mais os usuários utilizando a ferramenta.
Para se manter seguro dentro desse universo de aplicativos devem ser tomados alguns cuidados:

- Os aplicativos devem ser baixados pela loja oficial do sistema operacional. Aplicativos de lojas não oficiais podem ser fraudulentos.
- Antes de baixar algum aplicativo, é preciso verificar se as suas permissões são condizentes com o uso. Por exemplo, um app de jogo provavelmente não utilizará um microfone, então não existe necessidade de pedir a permissão para usá-lo.
- É importante acompanhar a classificação e as avaliações dos usuários. Normalmente, outros usuários já relatam ali os problemas encontrados nos apps.
- A quantidade de download do app também pode ser importante, pois normalmente apps com malware são achados pelas lojas oficiais mais facilmente e, se ele tiver muita avaliação e download, provavelmente ele será seguro.
- É importante verificar se o app tem fotos e vídeos com seu funcionamento na loja de apps.
- As lojas oficiais possuem histórico de atualizações. Apps bastante atualizados provavelmente conseguiram manter um nível de segurança maior.

É muito importante também que o usuário mantenha um nível de segurança básica no smartphone, tanto mantendo um bom Internet Security mobile caso o smartphone seja Android e tenha cuidado ao utilizar principalmente o e-mail e as redes sociais:

- E-mails desconhecidos não devem ser abertos, principalmente se tiverem anexos.
- E-mails fraudulentos que são imitações de e-mails de grandes empresas podem ser descobertos ao verificar o e-mail. Normalmente são e-mails bastante estranhos com caracteres que não façam sentido.
- Erros de português ou inglês são frequentes em e-mails fraudulentos.
- Nas redes sociais o marketing pode ser feito mostrando um produto com um valor bem abaixo do mercado, mas o nome é diferente da loja virtual conhecida, por exemplo, a loja conhecida é a “ABC” então o criminoso colocará o perfil de marketing com o nome “Saldão ABC”.

A Proteste e a Google possuem uma iniciativa com o objetivo de promover mais segurança na internet e conscientizar todos para a importância de proteger a privacidade do usuário na rede e essa parceria está disponível no canal ConectaJá da Proteste. Lá é possível encontrar dicas e informações de proteção para a sua conexão, dispositivos, contas e compras, além de auxiliar nas questões de privacidade e cuidados com as crianças e o uso dos seus dispositivos.

3. Referências

6 curiosidades sobre a história dos smartphone – Revista Galileu. Disponível em: <https://revistagalileu.globo.com/Tecnologia/noticia/2019/07/6-curiosidades-sobre-historia-dos-smartphones.html>. Acesso em: 06 de Abr de 2021.

Redes sociais – Toda Matéria. Disponível em: <https://www.todamateria.com.br/redes-sociais/>. Acesso em: 08 de Abr de 2021.

Facebook supera Orkut no Brasil com mais de 30 milhões de usuários. Disponível em: <http://www.folha1.com.br/_conteudo/2012/01/blogs/blogtech/221141-facebook-supera-orkut-no-brasil-com-mais-de-30-milhoes-de-usuarios.html>. Acesso em: 08 de Abr de 2021.

Social media usage in Brazil – Statista. Disponível em: <https://www.statista.com/topics/6949/social-media-usage-in-brazil/>. Acesso em: 08 de Abr de 2021.

Estatisticas TikTok – OBERLO. Disponível em: < https://www.oberlo.com.br/blog/estatisticas-tiktok>. Acesso em: 08 de Abr de 2021.

Security report 2018/2019 – AVTEST. Disponível em: <https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf>. Acesso em: 14 de Abr de 2021.

Aprenda sobre Malware e como proteger todos os seus dispositivos contra eles – Kaspersky. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>. Acesso em: 14 de Abr de 2021.

LGPD: 11 conceitos das leis de proteção de dados que você precisa conhecer – Assis e Mendes. Disponível em: <https://assisemendes.com.br/lgpd-conceitos/#:~:text=A%20LGPD%20aborda%20outros%20dois,na%20ocasi%C3%A3o%20de%20seu%20tratamento%E2%80%9D.>. Acesso em: 14 de Abr de 2021.

A nova lei de proteção de dados para pequenas e médias empresas – Proteste e Google. Disponível em:< https://conectaja.proteste.org.br/lgpdparapme/>. Acesso em: 14 de Abr. de 2021.
Websegura – Proteste e Google. Disponível em: < https://conectaja.proteste.org.br/websegura/index.html>. Acesso em: 14 de Abr. de 2021.

Shopping during the pandemic – IPSOS. Disponível em: < https://www.ipsos.com/sites/default/files/ct/news/documents/2021-01/shopping-during-the-pandemic.pdf>. Acesso em: 14 de Abr de 2021.

E-commerce brasileiro cresce 22,7% com faturamento de R$75 bi em 2019 – Ecommerce Brasil. Disponível em: https://www.ecommercebrasil.com.br/noticias/e-commerce-brasileiro-cresce-2019-compreconfie/ Acesso em 13 de Abril de 2021.

AMZDiscover. Disponível em: https://www.amzdiscover.com/blog/3-free-fake-reviews-detectors-to-help-you-spot-fake-reviews-on-amazon/ Acesso em: 12 de Abril de 2021.

Cuidado com as falsas avaliações – UOL. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/11/23/cuidado-com-as-falsas-avaliacoes-de-produtos-aprenda-a-detectar.htm Acesso em 15 de Abril de 2021.

Metalfloss. Disponível em: https://www.mentalfloss.com/article/582808/how-to-spot-fake-amazon-reviews Acesso em 16 de Abril de 2021.

ZDnet. Disponível em: https://www.zdnet.com/article/fake-reviews-facebook-and-ebay-ban-dozens-of-groups-after-watchdog-probe/ Acesso em 16 de Abril de 2021.

How many websites are there? – Statista. Disponível em: <https://www.statista.com/chart/19058/how-many-websites-are-there/>. Acesso em: 12 de Abr de 2021.

Brasil tem 134 milhões de usuários de internet – Agência Brasil. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em: 15 de Abr de 2021.

O que é um buscador? IC UFF. Disponível em: < http://www.ic.uff.br/~rosangela/Projeto%20site%20ENINED/buscador/buscador1.html#:~:text=Um%20mecanismo%20de%20busca%20ou-,palavras%2Dchave%20indicadas%20pelo%20usu%C3%A1rio.>. Acesso em: 14 de Abr. de 2021.

O que é Fake News e quais seus impactos? – Cia Websites. Disponível em: <https://www.ciawebsites.com.br/facebook/o-que-e-fake-news-e-quais-seus-impactos/#Por_que_uma_fake_news_e_um_problema>. Acesso em 13 de Abr. de 2021.

O que são Fake News? – Educa mais brasil. Disponível em: <https://www.educamaisbrasil.com.br/educacao/dicas/o-que-sao-fake-news>. Acesso em 13 de Abr. de 2021.

Saúde sem Fake News – Ministério da saúde. Disponível em: <https://antigo.saude.gov.br/fake-news/>. Acesso em: 13 de Abr. de 2021.

Procura por cursos online cresce durante período de quarentena. – Terra. Disponível em: <https://www.terra.com.br/noticias/dino/procura-por-cursos-online-cresce-durante-periodo-de-quarentena,c3bd2184c48535f25da13bdb80689302cugbza8i.html>. Acesso em: 13 de Abr. de 2021.

Como identificar um malware em aparelhos Android – Olhar digital. Disponível em: <https://olhardigital.com.br/2020/07/23/seguranca/como-identificar-um-malware-em-aparelhos-android/>. Acesso em 12 de Abr. de 2021.

Aplicativos potencialmente indesejados – ESET. Disponível em: <https://help.eset.com/glossary/pt-BR/unwanted_application.html>. Acesso em: 09 de Abr. de 2021.


PROTESTE
A NOSSA VOZ IMPÕE RESPEITO