12 things you should never do online

BY KOMANDO STAFF, KOMANDO.COM, SEPTEMBER 18, 2021

We all make silly mistakes sometimes. We answer robocalls (those numbers do look *awfully* familiar), click links we should have checked first, and open spam emails.

Everyone is vulnerable and can be caught off guard. It's what we do next that really counts. Do you believe the caller claiming to be an IRS employee, use your credit card on a sketchy site, or download files from a sender you don't recognize?

If you do, the consequences can be dire. That's why we've put together this list of 12 things you should never do online, along with do-it-yourself security tips, as reminders that we have to be vigilant with every click we make.

1. Don't give correct answers when setting up security questions

If this has you scratching your head, we get it. It might sound counterintuitive. But this simple trick keeps you one step ahead of cybercriminals.

Think about it this way: If someone knows personal details about you, they'll be able to answer these questions in a snap. Maybe a jealous former friend wants to wreak havoc on your accounts. Maybe a creepy cyberstalker has studied you for a while.

Or maybe a potential hacker randomly saw an opportunity to break into your accounts. Sadly, it's all too easy for them to collect all the personal information they need to answer those security questions accurately.

That's why you should throw potential invaders for a loop by picking incorrect answers for your security questions. By not giving the answers people will expect, you're taking away their ace in the hole.

It helps to think of cybersecurity like a chess game: You have to stay one step ahead of your opponent to win. Of course, you'll have to remember those answers.

2. Did an ad send you to a new site? Don't click any download buttons

So an ad worked. You were browsing, you saw an ad box with an intriguing item and you clicked on it. That takes you to a shiny new site with many more goodies you can buy.

Oh…and that site has ads, too. When it comes to ads, the internet is like the movie "Inception." There are dreams within dreams and ads within ads.

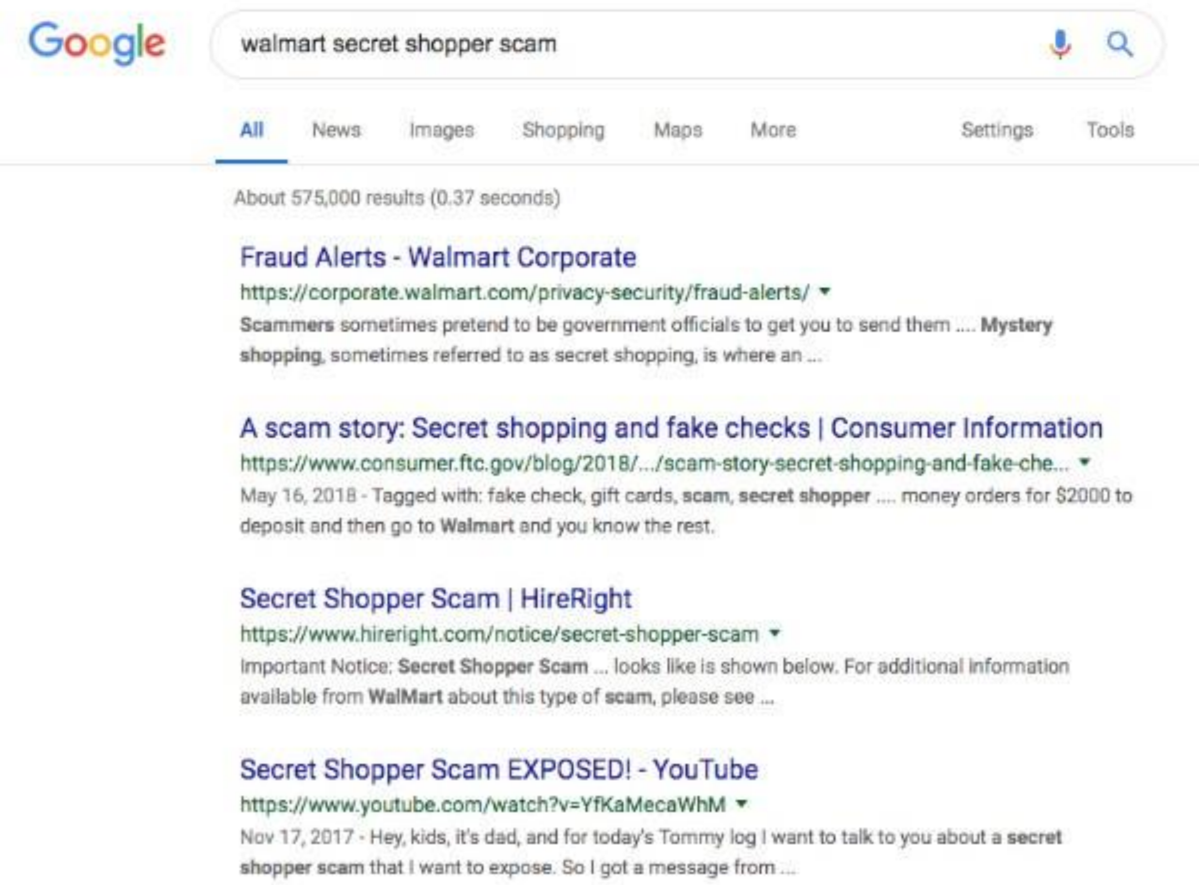
While you're here, don't download anything from that site. Remember that *anyone* can put out ads — and many sites won't properly investigate their partners. That means you could be browsing on a safe site and see an intriguing ad. Click it, and you might be taken to a new site filled with malware.

Generally, it's a good rule of thumb to avoid downloading when you can. On a related note, never download an ad. That's just inviting trouble.

3. Don't fall for fake posts

We've said this before, but it's worth repeating: If you get an email solicitation to participate in a survey or for a money-making opportunity you didn't sign up for, **don't click the links**. The same goes for work-from-home gigs that seem just a little too good to be true.

Open a browser window (Chrome, Safari, Firefox or whatever you use) and search for the company name plus the word "scam." Chances are, if it is a scam, someone else has reported it.



About 575,000 results (0.37 seconds)

Fraud Alerts - Walmart Corporate
https://corporate.walmart.com/privacy-security/fraud-alerts/
Scammers sometimes pretend to be government officials to get you to send them .... **Mystery shopping**, sometimes referred to as secret shopping, is where an ...

A scam story: Secret shopping and fake checks | Consumer Information
https://www.consumer.ftc.gov/blog/2018/.../scam-story-secret-shopping-and-fake-che...
May 16, 2018 - Tagged with: fake check, gift cards, **scam**, **secret shopper** .... money orders for $2000 to deposit and then go to **Walmart** and you know the rest.

Secret Shopper Scam | HireRight
https://www.hireright.com/notice/secret-shopper-scam
Important Notice: **Secret Shopper Scam** ... looks like is shown below. For additional information available from **WalMart** about this type of **scam**, please see ...

Secret Shopper Scam EXPOSED! - YouTube
https://www.youtube.com/watch?v=YfKaMecaWhM
Nov 17, 2017 - Hey, kids, it's dad, and for today's Tommy log I want to talk to you about a **secret shopper scam** that I want to expose. So I got a message from ...

If the email comes from what seems to be a real person, do a quick Google search (or use one of these **alternatives to Google**) for the person's name plus the company name. If you have a LinkedIn account, go there and search for the person and company, too.

That's a smart way to confirm the person emailing you works for the company they claim to. Check that the person posts regularly and is connected to others; those are signs the profile is real and not just a front.

4. Don't skip 2-factor authentication

Use **two-factor authentication** any time a website or app offers it. Yes, it involves a couple of extra steps, but the purpose is to protect you if someone tries to access your accounts from a device the website doesn't recognize.

Anyone who uses Facebook is already familiar with 2FA. If you use a work, public, friend or family's computer or new device to sign in, Facebook requires you to verify that it's really you, using 2FA.

This is a no-brainer for any financial account, and we recommend it for your email and any service that has your payment info, too.

DIY advice: **Use a 2FA authenticator app to protect your online accounts and cellphone number.**

5. Don't reuse passwords or password formulas

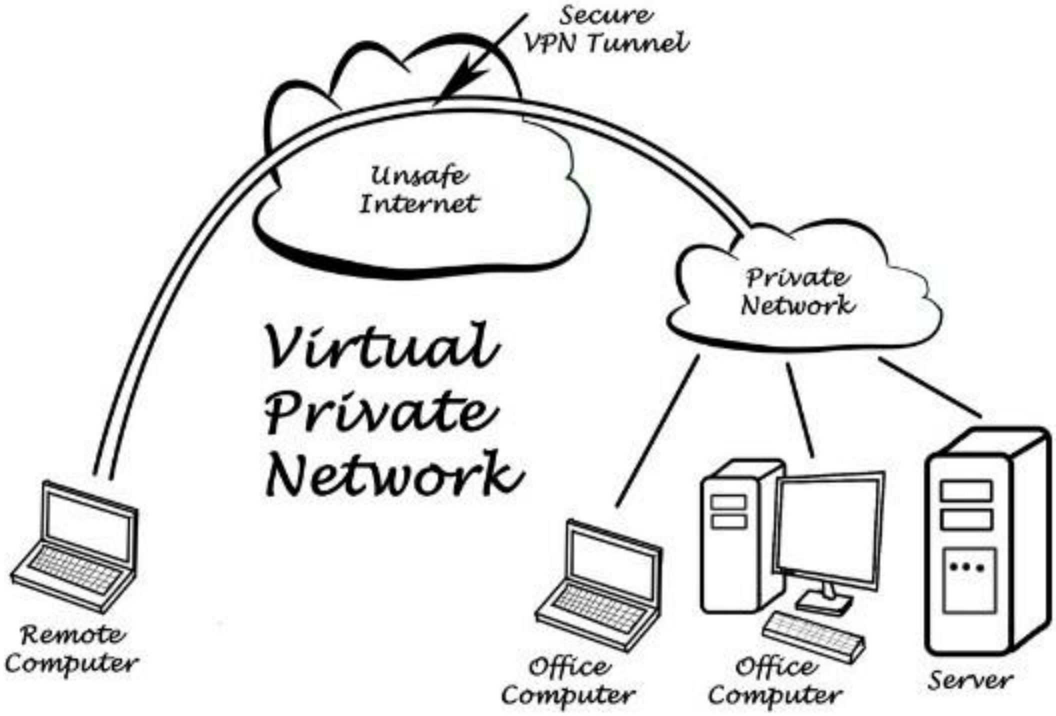
You'd never use a password like "123456," "abcd1234," or "password," right? If you don't use a password manager, how do you remember them all?

You don't write them down, store them on your computer or reuse them, do you? So, how do you safely store passwords, so you don't have to memorize them?

We don't recommend you use password formulas that are easy to hack, like "website+birthdate," as in google1225, adobe1225 or facebook1225. You can see how that'd be easy to crack.

DIY advice: Use a **safe and secure password manager**. You can also try a **free password generator**, which gives you crazy, impossible-to-hack-or-memorize passwords like *p6Us9temWz#B*. Or **let your browser do the work for you**.

6. Don't use public Wi-Fi



We know: Saying "Don't use public Wi-Fi" is like saying, "Don't go out in public." It's impossible. But you really should be careful about what you do on a public network. Save the banking for a trusted network, and be extra careful about the sites you visit and the links you click. Your best bet, though, is to use a VPN.

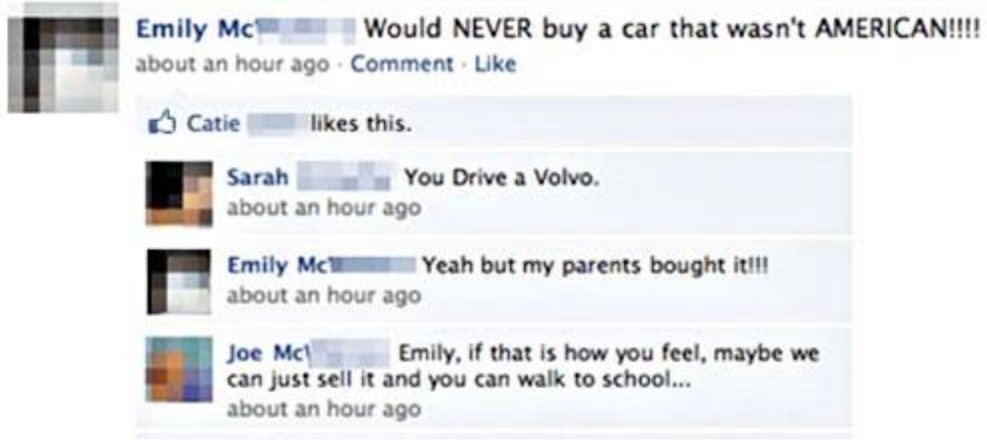
DIY advice: If you have to use public Wi-Fi, practice safe surfing. A VPN (virtual private network) which creates an encrypted connection through a secure server that allows you to browse the internet. Businesses have been using VPN technology for years, and more private users are adopting them as well.

Not really sure how VPNs work? No worries. **Tap or click for 6 questions about VPNs you've been afraid to ask**.

7. Don't fight on social media

Time and time again, research shows social media makes us depressed, angry and isolated. During the pandemic, we believed social media would bring us together, but really, we got sucked into scrolling through endless timelines, comments and arguments. **Tap or click for Kim's advice on how to step away.**

Plus, you might lose your car, like this girl almost did when her parents saw her complain about the car they bought for her.



Emily Mc[redacted] Would NEVER buy a car that wasn't AMERICAN!!!!
about an hour ago · Comment · Like

Catie [redacted] likes this.

Sarah [redacted] You Drive a Volvo.
about an hour ago

Emily Mc[redacted] Yeah but my parents bought it!!!
about an hour ago

Joe Mc[redacted] Emily, if that is how you feel, maybe we can just sell it and you can walk to school...
about an hour ago

Source: [someecards.com]

DIY advice: If you can't **break up with Facebook**, Twitter, Instagram, or whatever channel monopolizes your time and incites the scrapper in you, use common sense. Don't post anything that you wouldn't want your grandmother to see or that could come back and haunt you when you look for a job … or that some website would post as an example of what not to do online.

8. Don't post sensitive photos online

Speaking of not posting anything that could haunt you later, we're talking about things that may seem innocent, like photos of your kids or grandkids.

There's a whole conversation on the internet about whether or not parents should post photos of their kids online and share them publicly. In 20 years, will your children thank you for sharing their private lives with the world? One woman even sued her mother (and won) after she refused to take down photos of her grandchild.

Not to mention, **child predators set up fake social media profiles** and troll pages looking for innocent victims.

DIY advice: Change your privacy settings on **Facebook**, **Twitter and Google** so only your closest contacts can see your pictures. If you have kids at home, don't share full names or specific locations. Share only with people you actually know, check with other parents before sharing photos of their kids, and **wipe out hidden data from photos**.

9. Don't post vacation photos or updates while you're gone

If you venture out for a road trip or even just a day away, think twice before you post on social media.

It's so tempting to share in-the-moment updates and pictures while you're on vacation. Think of these as public announcements that say, "I'm out of town. My house is empty. Go burglarize me." Wait until you get back home and post your photos after the fact.

DIY advice: If you've got a home alarm system from our sponsor, **SimpliSafe**, you can monitor your property and get alerts when you are away. Thieves are less likely to break into homes that are protected by alarms, cameras and motion sensors. SimpliSafe is easy to install without having to call a professional. Visit **simplisafe.com/kim** for a great deal that Kim negotiated for you.

10. Never diagnose yourself on WebMD or similar sites

Let's say you have a persistent cough. When you searched online, you diagnosed yourself with pneumonia, tuberculosis, lung cancer, heart disease, acid reflux and chronic bronchitis. After all, those conditions share similar symptoms. You're freaked out.

Sites like WebMD, Mayo Clinic and Cleveland Clinic are packed full of good, reliable information, but that doesn't mean they should replace your doctors.

It's even more dangerous to use YouTube to look for medical information. Just like how conspiracy theory videos can dominate political searches on YouTube, health misinformation can climb to the top of your recommended videos and searches.

DIY advice: Leave the diagnosis to medical professionals. Use those **medical reference sites** to learn more about what your doctors tell you, and always consult with your doctor before beginning any medical treatment. Or consider setting up a virtual appointment. **Tap or click for our guide to getting started with telemedicine.**

11. Don't drunk shop online

Have you ever fired up your browser after a glass of wine or two? Apparently, **drunk shopping is a billion-dollar industry on Amazon**. A 2019 survey showed 79% of alcohol consumers have made at least one drunk purchase. Clothing and shoes are the most common drunk purchase.

DIY advice: **Set up spending alerts with your bank**. Most banks will allow you to set a dollar amount and if you go over that amount, you'll get a text message or email. That way, when you sober up in a few hours and check your messages, you'll have time to cancel your orders. As a bonus, if someone gets hold of your credit or bank card and makes purchases, you'll get alerts if they go over your limit.

12. Don't take quizzes online (especially on Facebook)

If you are logged into a website and take one of those tempting quizzes like, "Which 'Friends' character is your soulmate," you're potentially handing over personal information about you. When you take these quizzes, you're helping websites create profiles about you so they can sell your information and target you with advertisements.

And some quiz sites are downright sketchy. You never know who is watching what you type or what could happen when you hit submit.

DIY advice: Aside from the obvious "don't take a Facebook quiz," there are steps you can take to **disable third-party app access to your personal information.**