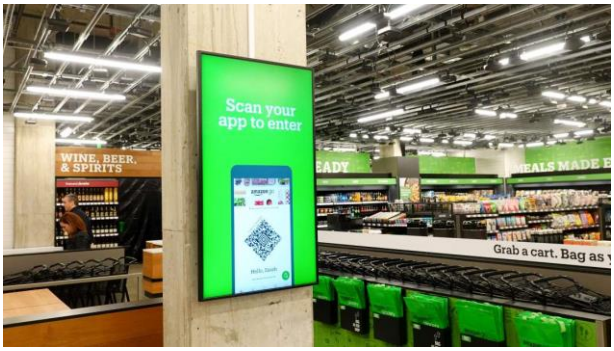
PayPal, passwords and Wi-Fi: 11 tips for better digital security

Jefferson Graham, USA TODAY 3 hrs ago

The data breach news this week was terrible, as usual.



© Jefferson Graham Interior of the new Amazon Go Grocery store, by Jefferson Graham

A company that works with many law enforcement agencies to track billions of photos through facial recognition got hacked really badly. It had its client list stolen.

A judge on ABC's Shark Tank is out nearly $400,000 after her assistant fell victim to a "phishing" scam.

PayPal, the payment app used by millions, was discovered to have a bug that led to (now fixed) unauthorized transactions.

And on and on it went.

Meanwhile, I spent two days this week talking to security professionals at the RSA Conference in San Francisco, where much of the activity focused on how to avoid getting hacked.

In response, I came up with my own 11-point plan to better protect myself against identity theft.

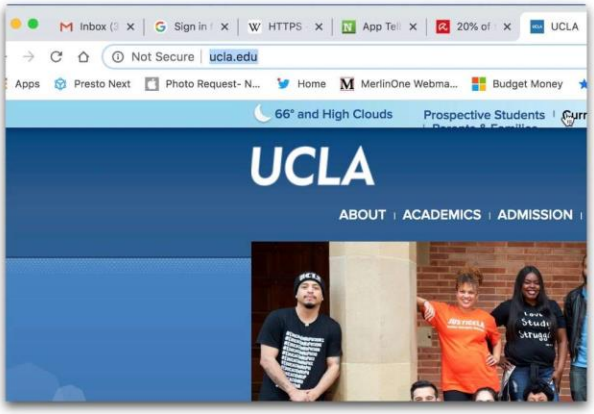
Will it work? Who knows. Is it better than doing nothing? Absolutely.

1. No hotel, coffee shop, airport Wi-FI

That's a given, right? We know how easy it is to hack into them. If you're looking up the price of a hotel room or reading the latest news from USA TODAY, then obviously free Wi-Fi is OK, but not for important stuff like banking. Unless you add in option No. 3. (See below.)

2. Check for https

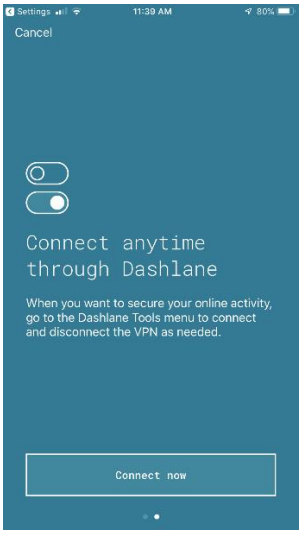
Trusted websites now feature an HTTPS protocol as the root address of the website, which basically means the website is encrypted. You'll know you're not at an HTTPS site because Google Chrome will trumpet for you that it's "Not secure" at the top of the page. So what to do, say, if you want to read the news on the Drudge Report or check out the offeri at UCLA.edu?



© screenshot UCLA has a non-secure website that doesn't use the HTTPS protocol

3. Get a VPN

That stands for virtual private network, and it encrypts your data and makes it somewhat private, making it safer to surf, even in free Wi-Fi zones. (You're on the internet, after all.) VPNs charge monthly to use their services. ExpressVPN, which Tom's Guide selected as its top pick, is $13 monthly unless you commit to a year. Do so, and the charge is $6.67 monthly.



© Screenshot Dashlane's VPN feature

4. Use password managers

These programs, from companies like Dashlane, LastPass and 1Password, keep track of your many passwords and also provide software for you to store your credit cards. Say you are in a free Wi-Fi zone and have ignored my recommendations. Normally, I'd say ditch typing in your credit card information here because someone could pick up the keystrokes. But with the Dashlane app, the numbers are transmitted electronically, without any typing. Additionally, Dashlane now comes with built-in VPN, and rates start at $4.99 monthly.

5. Use two-factor authentication

Speaking of passwords, one thing we're told to do often is to move to two-factor authentication, to input two passwords instead of one as a more effective way to keep hackers away. But the fact is, most of us refuse to do it because it's hard enough typing in one password. Who wants to wait for a code to show up and have to do it again? Google has a good solution in prompts. Instead of making you type in a code, it simply sends you a message and asks if you want to sign in. You confirm, and you're in.

6. Update software

You hear it all the time. Accept every software update. They are issued to keep your system more robust and up to date. It's not just the operating system on your computer and phone that need to be updated. It's everything, says Robert Lipovsky, a senior malware researcher for security firm ESET. So don't leave out your network router and internet devices at home like the Ring doorbell and Nest thermostat as well.

7. Don't sign in with Facebook

Many of us hate the log-in and password process so much that we take the lazy way out. Meaning when the website asks us if we'd like to sign in with our Facebook credentials instead, we eagerly say yes. Don't do it. According to a study by Princeton, you're giving up a lot. Third-party trackers can pick up tons of personal information when you do this, which is not something you signed up for.

8. Skip Venmo

The popular digital payment app also sends your geographic location and associations to a data-mining firm called Braze. I've switched to PayPal, which ironically, owns Venmo, yet operates in a less grabby fashion.

9. Be wary of email links

This is a given, right? You get an e-mail, it looks authentic, and in it is a request to click a link to confirm your account. Before you do this (please don't) check the e-mail address to see if it was really written by the company it claims to be. Usually, it's not the case. See my line by line takedown of a fake Chase Bank phishing email that I posted recently. And in the case of Shark Tank's Barbara Corcoran, her bookkeeper got hoodwinked by a bogus email that looked like it was from Corcoran's assistant. "Think before you click," says Robert Lipovsky, a senior malware researcher for security firm ESET.

10. Beware fake voice calls

I learned at RSA that phishing e-mails are still the No. 1 way to try to steal your identity but that growing is fake audio. The boss appears to call and demands you wire money immediately to a vendor. Call the boss back before you do anything. “This is a threat that’s waiting to happen,” says says Vijay Balasubramaniyan, CEO of Pindrop, a company that offers biometric authentication for businesses. “It’s a very small number now, but it’s very real.”

© screenshot After signing up for the Community text service, actress Kerry Washington gets entered into a contact list

11. Fill out contact lists on your phone

So when the boss does call, the correct number will match the name. Additionally, if you have a good, robust contact list, you'll only answer calls from known contacts and be able to skip robocalls. Apple has a new feature in the iOS13 software that sends all non-contact calls directly to voicemail.

How sweet is that?

In other tech news this week

Amazon opened the grocery store of the future in Seattle this week. The just-over-10,000-square-foot facility is about 25% the size of the average supermarket but has a fuller selection than the 7-Eleven-sized original Go stores. The selling proposition: no long lines at the cash register because Amazon's cameras and sensors can detect your selections and charge your app accordingly. In response, the president of a union representing grocery workers called the concept a job killer.