Why you should never use someone else's Apple ID on your iPhone, according to Kaspersky Lab

Users of any Apple device must have an Apple ID. It's a kind of digital passport for journeying in Appleland. You need an Apple ID to enter, and it gives you certain rights. And it should be treated like a passport: Don't lend it to anyone, and don't borrow anyone else's.

The first point is obvious. Giving someone your Apple ID means losing access to your own devices, your data, your subscriptions and so on. But questions often arise about why you should never enter someone else's Apple ID on your iPhone or iPad. Let's use Marcie's story as a case study.

Selling an iPhone
After a year of tender loving care, Marcie decided to sell her iPhone X. It was so last-year, she simply had to upgrade to the XS, or at least the XR. Her first thought was eBay, plus an ad on Craigslist for good measure.

Next came the question of price. The phone was in good shape, so she decided to aim high. She hadn't spent a year blowing dust off it for nothing. And not a single scratch! Sure, it might take a while to find a buyer, but Marcie was in no hurry.

To her surprise, one appeared the very next day. A polite woman wrote that her husband really wanted to buy the iPhone, but he was terribly busy and couldn't drop by until the end of the week. But he really liked the fact that the device was in perfect condition, so he wanted to make an advance payment and pick it up later. To check that the phone really was A-OK, the woman asked Marcie to enter her husband's Apple ID into the device. If it worked, she would transfer the prepayment right there and then.

Marcie was beaming — she'd expected to wait at least a couple of weeks, but 24 hours later, it was all done. The woman had sent her husband's Apple ID e-mail and password. Marcie wondered why these people were so carefree about giving such valuable data to a total stranger. But that was not her problem, so she entered the information into the phone and informed the woman that everything was ready to be checked.

And then something happened that Marcie wasn't expecting at all. A message appeared on the iPhone screen saying that the device was blocked, and that someone at such-and-such e-mail address had to be contacted to unblock it. There was no way past the black screen with its unpleasant tidings; the phone was blocked, period.

The "polite woman" (read: fake account) no longer replied to Marcie's messages. So Marcie wrote to the e-mail address provided, only to be informed that to get her phone unblocked, she would have to transfer a tidy sum in cryptocurrency.

Marcie paused to think — there was no guarantee she wouldn't be deceived a second time. The iPhone itself was lying on the table like a useless brick, totally indifferent to Marcie's inner turmoil. Besides being unsure about whether to pay, she was angry with herself for being so easily duped.

Beware of strangers bearing Apple IDs

As soon as you let someone enter their Apple ID on your Apple device, you effectively relinquish possession of it. And if that someone is a cybercriminal, they will not let go easily: having hoodwinked the victim, they block the device using the “Find my iPhone” feature in iCloud.

This feature is intended to prevent a stranger who has found your lost phone from freely perusing its contents, and to display your contacts on the screen so the finder can contact you and return the phone.

In this case, of course, the device was not lost. But as soon as the victim enters another person’s Apple ID, the iPhone is immediately added to that person’s list of associated devices in iCloud, and henceforth can do anything they like with it. Thus, a handy feature can serve nefarious purposes: Cybercriminals can use it to block iPhones and iPads — and then demand a ransom.

So you should take care when selling used devices, but that’s not the only case. A favorite social engineering technique among scammers is to cozy up to users of Apple-related forums, and then ask to enter their Apple ID under various pretexts like “my phone’s dead, my contacts are in iCloud, gotta call my boss urgently, please help,” or something in that vein.

But surely if you know the cybercriminals’ Apple ID e-mail and password, you can just log in to the Web version of iCloud and put things right? Nope. The fraudsters’ account is protected with two-factor authentication, so to log into their iCloud, you also need to enter the code sent to one of their devices. Naturally, only they have access to their devices, so simply knowing their Apple ID isn’t enough.

The moral of the story: Never enter someone else’s Apple ID on your device. Even if they say please.