Issued 3/28/18

Your Online Identity Sells for $1,170 on the Dark Web -- Here's How to Block the Sale

Harvesting a few of your credit cards, your social security number, your billing address, and even the names of your children now has an exact price tag, almost like an Amazon shopping list. According to a new study by Privacy Central, it's exactly $1,170 on the dark web. Netflix accounts, an Uber login, and access to your AirBnB credentials come cheap -- $10 each. And, how about your Gmail login? That sells for about a dollar. How about your iTunes account info? That's exactly $15.38. PayPal account? $247. Security experts suggest the laundry list of items for sale is only going to grow -- and get more affordable. Daniel Smith, a security researcher at Radware, says dark web hackers tend to offer package deals, one that might include your mother's maiden name as a bonus. The listings are getting more and more sophisticated, and the prices are driven by recent data breaches. "Credit cards typically sell between $5 to $20 per card, depending on the value of the card. When large databases go up for sale on the darknet, records drop to under a dollar a piece." "We have seen prices as low as $100 for two credit cards and even $350 for ten cards," added Mounir Hahad, the Head of Threat Research at Juniper Networks. "We have also seen $10 for a keylogger malware, which will capture passwords from any computer you have access to - $40 can often get you access to the social media accounts of anyone you're interested in." Smith says one of the main ways hackers steal your identity these days is through phishing scams, those troubling ploys that trick you into giving out bank details, logins, and your social security number. The emails look legitimate, as though Bank of America or Wells Fargo really are having a computer glitch and need you to fill out an online form. His advice?

Never reply to an email that looks sketchy, since 93 percent of phishing scams are meant to steal your personally identifiable information. Freezing or closing all accounts you don't use, reporting fraudulent activity to your bank and to the FTC, and staying vigilant all help. "Always verify the company that you are doing business," Smith said. "In the end, if you suspect that you are a victim of fraud, report it to the authorities right away." Even the most advanced security measures don't seem to stop hackers. "There's not much consumers can do. The best you can do is put credit freeze and a hold on things and hold on tight. This is going to get worse."