

02/11/2014

By Adam Levin

Regular viewers of MTV's series "Catfish" (in which online-only, deceptive relationships are pulled into the real world, albeit with cameras running) might think that the show just highlights the extreme cases of a common problem – people who tell lies in search of a personal connection. For instance, studies show that about 81% of people [lie](#) in their online dating profiles and everyone has a story about a deceptive boyfriend or girlfriend who wasn't everything they initially seemed.

But lying about who you are – and your affections – solely to get access to someone else's personally identifying information or money is a more dangerous form of catfishing not often highlighted by the show, and it's on the rise just in time for Valentine's Day. In fact, we might as well officially call this phenomenon "catphishing," and add it to the growing roster of other notable [phishing scams](#).

The most famous catfishing victim, Notre Dame football star Manti Te'o, didn't lose much more than his pride in his ordeal, but other victims haven't been quite so lucky. Former Denver Nuggets star Chris Anderson faced a criminal investigation after a woman pretended to be him online and scammed and blackmailed more than a dozen victims (including a woman with whom he had a real-life relationship). A mother-daughter team in Colorado peeled more than \$1 million out of more than 300 women around the world pretending to be U.S. military men who just needed a little bit of cash to buy a phone or a plane ticket.

As the Better Business Bureau has noted, these [scams](#) are on the rise in part because they don't cost the scammers very much. Many online dating sites are free to users, fake photos are easy to find and a little investment – like in flower deliveries, which don't require the person ordering be present – can net more in financial returns from the charmed women or men who fall under a catfisher's spell.

So how do you make yourself less vulnerable to catfishing? Psychologist Jack Schafer warns

people to be wary of truth bias, or our innate belief that most people are telling us the truth in the absence of evidence to the contrary.

But there are some more concrete tips you can follow if you want to be safe from catfishers.

1. Be wary of romantic interest from someone who says they can't meet.

He's really American but lives abroad right now (but is using OKCupid and contacting people in your city). Her phone got shut off. His webcam won't work. Scammers have 100 arrows in their quiver of reasons you can't meet in person, talk on the phone or even see each other virtually and they're almost all disguising the fact that they're using another person's picture and a made-up identity to woo you. Before you let yourself get too sucked into a whirlwind romance with a would-be Romeo or Juliet, make sure the person you think you're falling for is more than just a few ghost-written love letters and a model's picture.

2. Be suspicious of someone who always has emergencies.

Once a catfisher thinks she or he has a live one on the line, they'll test their mark to see how far they can push the trust they've worked to establish. (It doesn't hurt that this can play into their efforts to avoid actually having to meet, talk or be seen.) But while having emergencies is a fact of life, involving people who don't really know you in them really isn't – and asking for money to resolve them is definitely not.

3. Never turn over personal information or pictures you wouldn't want widely seen.

Maybe your new love interest will suddenly ask for a credit card number to buy a plane ticket, or ask where your bank is or request something like your Social Security or passport number. Maybe they'll ask you for pictures of yourself in compromising situations, or to engage in some NSFW video chats. While giving out your personal information is enough of an identity danger, don't ignore the increased risk of having your personal pictures or screengrabs used as a form of actual blackmail by a catfisher out for more than just titillation.

4. Don't give someone money, or help him or her to access money.

Given that the whole point for many catfishers is to get money out of people, alarm bells should start going off the moment any potential romantic partner asks for even a little financial assistance. The first ask might be small – perhaps something to help take care of the emergency situation – but most catfishers will quickly accelerate their requests or demands for money as quickly as possible. If you don't help, they might ask you to deposit a check or accept a wire transfer from a friend and pass the money along, but the money you're supposed to get never really arrives. Don't do it!

5. Never click strange links or download files you receive.

Even the most heartfelt-seeming e-card can mask something more dangerous than an online-only romance: weird links to unfamiliar sites or files you're asked to download can contain malware or viruses that can do more than just spam your computer with ads. You could end up with a keystroke logger on your system, which would allow the sender to see passwords to everything (including your checking account), or a virus that turns your computer into a botnet to launch attacks against other sites. If you don't really know the person, don't trust the file (and, sometimes, even if you do know the person, don't trust the file).

Finally, if you think someone you've had an elusive online relationship has gotten hold of your personal information, it's extremely important that you check all of your financial accounts, regularly, for unauthorized charges. You should also check your credit reports, which you can get for [free](#) every year from each of the major credit reporting agencies, for accounts that you didn't open, or other signs that someone has been using your information for their own gain.

Valentine's Day is a high-pressure holiday for many people, and we've all been in situations where our foolish hearts trump our ability to see through a scam. But when that tiny alarm bell starts going off in your head, listen to it – and you will save both your heart and your hard-earned money.

Adam Levin is chairman and co-founder of Credit.com and Identity Theft 911. His experience as former director of the New Jersey Division of Consumer Affairs gives him unique insight into consumer privacy, legislation and financial advocacy. He is a nationally recognized expert on

identity theft and credit.