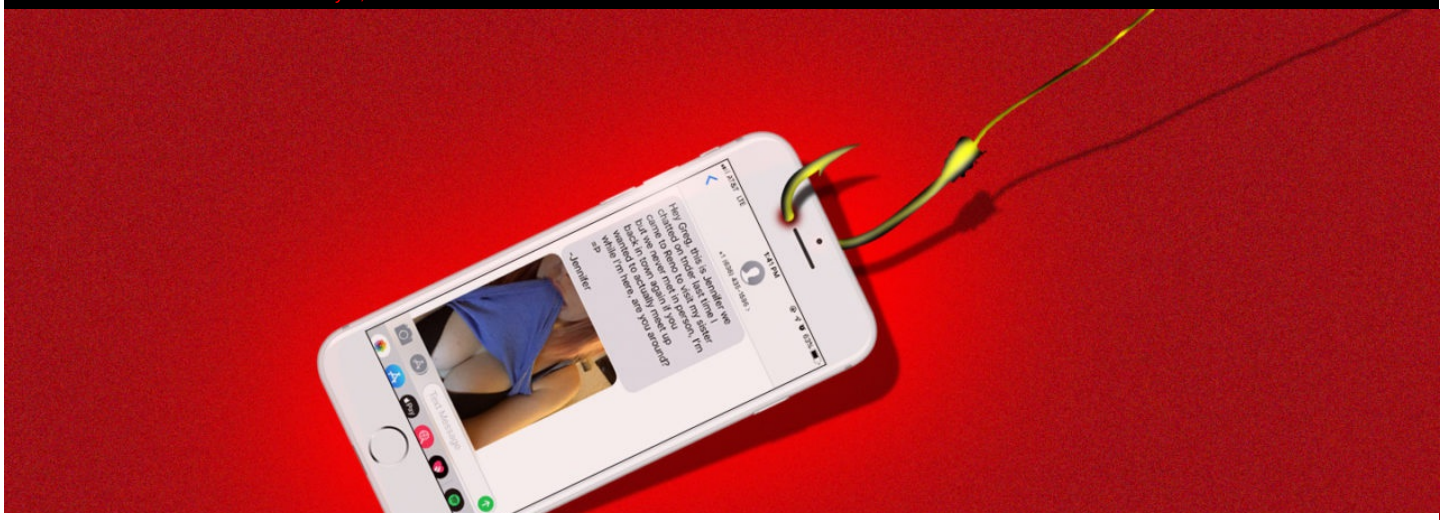
CULTURE Andrew Fiouzi / February 1, 2019



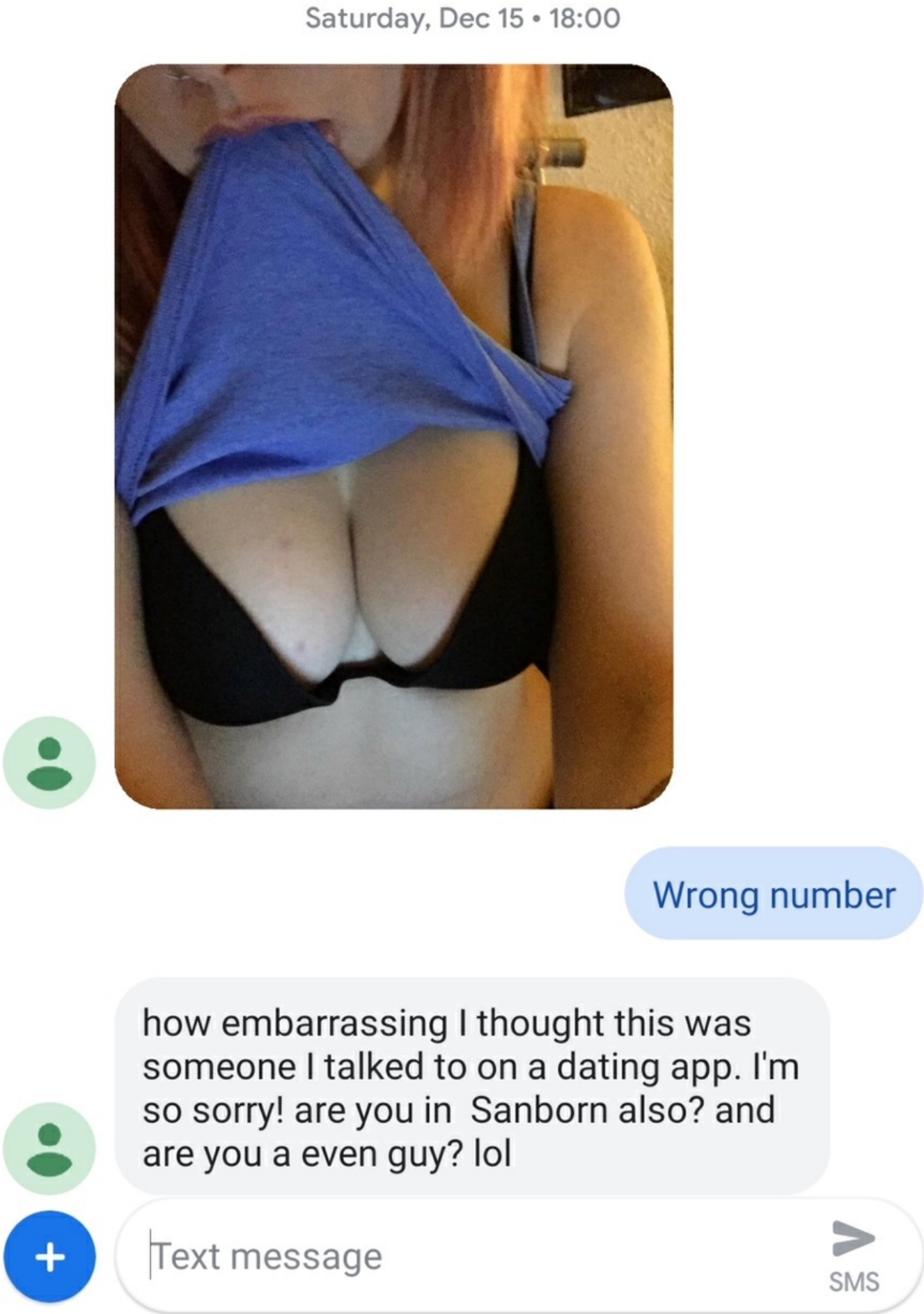
HACKERS ARE 'SMISH'-ING VICTIMS WITH BOOBS — TO THE TUNE OF BILLIONS OF DOLLARS

According to former federal agents, the surprise topless text is the next big evolution of scamming

Nothing screams "scam" like an unsolicited boob-flash pic from a random woman. The infamous male equivalent has become an epidemic: According to *Bustle*, 78 percent of the millennial women who've received a dick pic never asked for them. But pictures of boobs from women you've never met? That just doesn't happen.

And yet, there I was on a Sunday morning, lying next to my girlfriend, when I received a text message from "Jen," re-introducing herself (she claimed we'd already met on some dating app) by way of lifting up her shirt for a below-the-neck selfie.

I, regrettably (as I would later find out), responded to let her know that she had the wrong number before showing the exchange to my girlfriend, who was somewhat more bemused by the subterfuge than I. Undeterred by the mixup, Jen messaged me back to ask if I was "even a guy." My girlfriend, realizing something fishy was afoot, took my phone, complimented Jen on her breasts and facetiously criticized her for not being more cautious about sending cleavage pics to someone she didn't know. Jen, to her credit, really didn't give a shit — she ignored my girlfriend's advice and proposed — with an unforgivable number of spelling and grammatical errors — that we all meet up.



It was at this point — not considering that I would later investigate the circumstances of the exchange for this story — that I blocked the number and deleted the conversation from my phone. Because, y'know, let sleeping dogs lie… dead, preferably.

And that, I figured, was that.

At least, until I spoke to Thomas Martin, a former supervisory federal agent who represented the Department of Justice in more than 50 countries and who now runs his own private-investigation firm that employs former federal agents like himself. Martin told me that he had recently received nearly 100 calls from friends, family, clients and a couple of concerned wives who had asked about exactly this sort of salacious text message. “This particular scam is all done through texting and that’s the unique part of it,” said Martin.

As per this 2018 *USA Today* report, text message scams are referred to as “smishing” scams. “Similar to a ‘phishing’ scam — where computer users receive an authentic-looking email that appears to be from their bank, Internet Service Provider, favorite store or other organization – ‘smishing’ messages are sent to you via SMS (text message) on your mobile phone,” writes Marc Saltzman. “Cybercriminals are trying to lure you into providing account information — such as a login name, password or credit card info — by tapping on a link that takes you to a web site. Here they can get enough info to steal your identity. Or you might be asked to answer questions via text message or advised to call a phone number.”

If you’re thinking that only an idiot would be dumb enough to get scammed like this via text message, you’re the one being naive. An FBI fraud report from July states that victims of phishing scams suffered more tahn $12.5 billion in losses between October 2013 and May 2018. “In that time frame, the FBI counts 41,058 total U.S. victims who collectively lost at least $2.9 billion,” reports Bank Info Security.

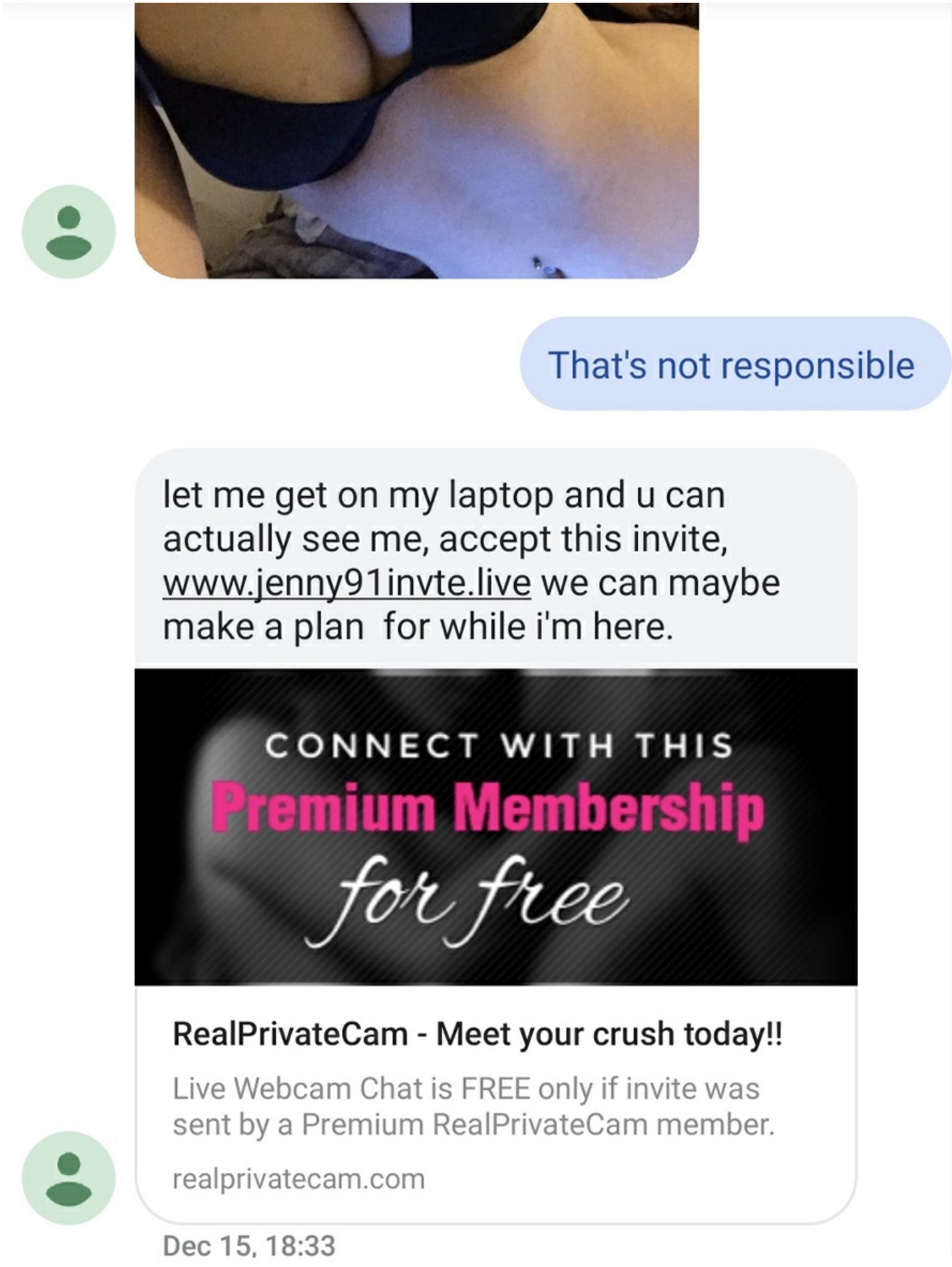
As for how this could possibly be true, a 2014 study on scam compliance and the psychology of persuasion found that there are certain characteristics that people who are victims of scams seem to share: A lack of self-control; trust in authority; a desire to act in the same way as our friends; or a tendency to act in a consistent way. According to the study’s author, David Modic, who researches the psychology of internet fraud at the University of Cambridge, there are a variety of ways that scammers gain a victim’s trust. “Modic points out, for instance, that some scammers gain a victim’s trust by pretending to share a mutual friend,” reports the BBC. “In other situations the scammer might contact the victim under the guise of a figure of authority — a doctor or a lawyer — to appear more persuasive. There are also scams that initially involve no loss of money and which are designed to encourage a victim to behave in a certain way, so that later they are more likely to behave in the same way when their money is at stake.”

Whatever the reason, the amount of money involved here seems like it should be enough to give the federal government cause to get involved and protect people against such attacks. But that’s not the case: Currently, only 23 states and Guam have laws specifically aimed at phishing schemes, while “other states have laws that address computer crime, fraudulent or deceptive practices or identity theft, which could also apply to phishing crimes,” per NCSL.org. There is no specific federal legislation pertaining strictly to phishing activities. “Originally, the Anti-Phishing Act of 2004 and the Anti-Phishing Act of 2005 would have imposed steeper penalties on those convicted of phishing activities, but the bills ultimately died in a subcommittee and were never enacted,” reports InfoSec Institute.

Even if there were federal laws that imposed severe punishments for cybercriminals, Martin isn’t convinced many of them would ever get caught. “Mueller’s indicted 12 Russians responsible for the phishing attacks on Americans during the 2016 election,” said Martin. “How many of those guys have been brought in? If you think you’re going to get some hacker living in the Cayman Islands, you’re living in the fairy tale dream.” He’s right, of course — it’s hard enough to successfully prosecute a cyber criminal if they live in the same country as the victim, so when that’s not the case, it’s close to impossible. “Many times we successfully collect good legal evidence and even verify the identity and location of the cyber criminal, but we have no legal ability to arrest the person,” writes Roger A. Grimes for *CSO*, an online magazine that addresses all security disciplines.

So what’s new about this boob-led approach? In the past, smishing scams usually began with an unexpected text message, appearing to be from your bank, informing you that you’ve been hacked. “The message will tell you to reply or ‘text back’ in order to reactivate your account,” reports *Thought Co*. “Other smishing scam text messages may include a link to a website you need to visit in order to resolve some non-existent problem.” The ultimate goal either way, naturally, being to convince you to

enter your banking information in order to swindle you out of your money.



That’s exactly what I’d assumed was happening the moment that well-filled bra first popped up on my phone, but Martin tells me he believes this new smishing technique is a little more advanced than your typical bot scam. “They’re definitely real people texting you back because of the way it’s set up,” he explains. “The number is some burner phone number that nobody’s ever going to be able to trace. The responses are not bot-lies.They come intermittently, they’re more sophisticated and their end

goal is to keep you talking."

Dispatched by "serious players," he adds, the scam is triggered the moment you respond. "It lets them know that you're an actual person," he says. "So once you signal them back, they have the malware to get into your phone, and from there, they can find your home address, your business address, your photos, your emails and your texts."

This is why he cautions against even opening the text message in the first place and blocking the number before deleting the conversation altogether. Realizing that I'd made myself vulnerable via a few seemingly innocuous texts, I ask Martin how much time I had before the other "Andrew Fiouzi" popped up in Nigeria, purchasing a truck load of flat-screen TVs. "They may not think that you're worthy of it," Martin explains. "I mean, knowing that you're a reporter, they may take some glee in that. I would definitely call Equifax, TransUnion and Experian, the three credit bureaus, and just say, 'I think I've been hacked,' and put a fraud alert on there, so they will contact you."

All that work, just because I thought it would be funny to mess with what I assumed was a bot.

Martin uses the analogy of an office building to explain the various levels of infiltration possible by way of your phone. "Let's suppose that you have a three-storey office building, or four, five or whatever. So you've now opened the door [by responding to the text message] and let them in. Now, it all depends on, do they want to go into the first floor and go to every office and tear through desks? Do they want to go to the second floor? Do they want to go to the third floor? It's all a sense of what they want to do." In other words, the longer you continue the text conversation before blocking the phone number and deleting it, the more susceptible you leave yourself to an electronic home invasion.

But again, this particular scam seemed a little different to Martin — no one had yet been prompted with a link asking for money. "At the end of the day, they're trying to get into your cell phone," says Martin. "I mean, why do this and not ask for money? It doesn't make any sense. The better deal is that they could probably make more money by getting your identifying data, getting into your bank accounts or getting into your credit. Or go into your photos, get into your emails or texts."

Put another way, Martin was considering the possibility that this scam, being more sophisticated than those he'd seen in the past, could be building toward an all-out financial assault. Because while most scammers plan to use the information they uncover from your phone to extort their victims in some way, in not one of the nearly 100 cases that Martin had seen so far had the hackers requested so much as an email address, or prompted anyone for any sort of payment. "That's the puzzling part about this thing," he says. "What we have come to learn — and I think we're the only ones who have had enough experience in this regard — is that their goal so far is to create chaos."

To what end, though? Martin admits that, since the hackers haven't shown their true intentions yet, he still wasn't sure exactly what they were after, so he hadn't ruled out any possibilities. "I don't *think* it's a Russian conspiracy to disrupt American people's lives, but that could possibly be down the road," he says, hastening to add that he's not a conspiracy theorist. People sharing their experience of receiving the text on Reddit were likewise baffled, noting that they, too, have never seen a scam like this. "In all of my years, I've never once had a spam message like that. What would be the motivation? Usually spam texts are convincing you to buy something or to advertise something," writes fallonharrod.

As it would later transpire, though, the answer may be relatively straightforward — and familiar — after all. "Basically, it's a mix between a scam and a marketing scheme, apparently designed to drive the textee to particular channels on a camming site," writes Filipa Ioannou, a reporter at *SFGate* who wrote about the scam earlier this month. Ioannou explains to me over the phone that she's had a few friends receive the same text with the same unsolicited photo, "All within the past three to four months," she says. Ioannou tells me that she looked on as one of her male friends continued down this salacious message scam rabbit hole — "It seems to take about half an hour to run through the program," she says — at which point one of her friends received a second, slightly different image of the bra-clad breasts, and finally, an individualized link to the site itself: RealPrivateCam.com (for your own sake, it's best you don't click that link).

Per its website, Real Private Cam is ostensibly a place where locals can connect with each other via "encrypted webcams."

According to online identity provider WhoIs.com, this domain was registered on April 25, 2018, and is set to expire on April 25, 2019. Strangely, although the website is indexed by Google, if you search for it, you'll find that Google has no information available for the page because, according to them, the website has "prevented Google from creating a page description, but didn't actually hide the page from Google."

As for who this website is targeting, based on a small sample size of Ioannou's friends, twoReddit threads and Martin's clients, most of the people who have admitted to receiving this picture of a random bra-clad woman via text message are men, as you might expect. (There is, however, at least one woman who claims to have received the same breast-y message: "I've gotten the same types of texts! And I'm a woman. Fortunately the fiancé trusts me and believed it was spam," writes this redditor). Targeting dudes with boobs isn't as sure a bet as you might think, though —while little is known about how gender predicts the likelihood of being scammed, one small study of an Australian population found that 40 percent of men had been scammed by romance scams, compared with 60 percent of women.

To become a member of the supposed camming site, you have to enter a few personal details, but not necessarily ones that would immediately raise giant red flags, like your social security number or bank card numbers — it asks instead for your full name, your zip code, your birth date and your gender. Intrigued as to what hackers may be able to do with this information, I reach back out to Martin nearly two weeks after our initial call, to ask just how much trouble I'd be in for if, for the sake of the story (honestly!), I gave the site that information about myself.

As it turns out, Martin has uncovered a lot more in that short time, reaching roughly the same conclusions as Ioannou. "If you go there and give your info, you're never going to hear back from them again," Martin tells me. "When they have your name and your date of birth, they can narrow down your identity to a handful of people. Once they have your zip code, they know exactly who you are. In [a client of Martin's] case, the hackers were able to take out a line of credit — they used it down in Jamaica to buy an iPad."

So there it was — the scam, fully actualized and almost disappointingly mundane. "[It's] kind of a shift from what we all originally thought," says Martin, who still seems at least somewhat convinced there's perhaps more to this scam that has yet to unfold.

But of course, as of writing this, "Jen's" boob scam is nearly two months old, and therefore, it's already old scam news. "The new one is targeting doctors and dentists," says Martin. "These guys are taking out loans for 'medical equipment' under the doctor's name. Lines of credit for $17,000, $18,000, $19,000. And they'll keep racking it up because no one's going to be able to find them."

And maybe that in and of itself is the scam within the scam — the galaxy brain scam, if you will. Because by the time anyone — even a PI unit staffed with former federal agents — begins to pull back the first layer of one cyber-con, the scammers have already ditched their burner phones and dialed up the next one.

Andrew Fiouzi

Andrew Fiouzi is a staff writer at MEL.