Moving Fraud: Be Careful if You're Moving to a New Home

September HackTalk: From bait-and-switch estimates to movers holding your belongings hostage, there has been an uptick in fraudulent activity during the vulnerable time when people are relocating. Watch out for these red flags.

HackTalk is a long-running monthly podcast with Sean Bailey and Devin Kropp, co-authors of Hack-Proof Your Life Now!, which covers the latest cybersecurity threats and issues advisors need to know to protect themselves and their clients.

Sean Bailey: Everyone, welcome back to our latest episode of HackTalk. I'm Sean Bailey, editor-in-chief at Horsesmouth. I'm here with Devin Kropp, co-author and co-creator of the *Savvy Cybersecurity Program* and *Hack Proof Your Life Now*.

Devin, What is going on in the world of cybersecurity, fraud and scams this month?

Devin Kropp: So, this month we are focusing on a scam that's not so cyber-related, but I think is still important for people to be aware of, and that is moving scams. So yes, we're talking about when you're physically moving from one home to another and using a moving company.

Unfortunately, there are people out there who are taking advantage of an already stressful, time-consuming situation and scamming people who are looking to move their items from one home to the next. And so we want to talk today a little bit about what to be on the lookout for if you are moving or you know someone who is moving, what these scams look like and the red flags that might alert you that something is off during the hiring or researching process.

Sean: I remember back in the day, as they say, there used to be this huge truck, it was called Mayflower. And whenever you come home from school and you see a Mayflower truck on the street, it was always cause of either great concern or great interest, depending on which way they were going.

Today there's all sorts of independent people who provide moving services, so you're not buying a trusted brand… What exactly is happening there?

Devin: There are a couple different scams we're seeing here. As you were saying, there are a ton of moving companies out there now, especially in city areas. I'm here in Brooklyn. I probably see a different moving company van every single day. And it can be hard to know who to use and what's a legitimate moving company.

So, some of the scams that we do see, probably one of the scariest is that you'll hire a moving company online. You start the process online. Maybe you pay a deposit. The truck shows up, it loads all your stuff onto it. You go to your new home to meet them and that moving truck never shows up. And they basically demand money, more money than you originally agreed to, to drop your items off. So essentially, they're holding your items hostage until you pay more money.

Sometimes they'll charge fees that weren't included in the original quote. Or they'll say, "You had more items than we agreed upon, and so you need to pay this money before we're going to drop your stuff off."

And when you're in that situation, what is one to do? You need your stuff. You're in your new home. It's empty because you don't have any of your furniture. So people end up usually paying to get them to show up and end up spending way more money than they had agreed upon initially. So that is probably the most severe example of moving scams.

Sean: Like an extortion, basically.

Devin: Yeah. And I think that's rarer than some of the other ones we're going to talk about, but that's the extreme of what could happen to you if you unfortunately go with a company that doesn't have your best interests in mind here.

Some of the more common things I think we see are companies who will provide you a kind of unrealistic low estimate at the beginning of the process, and then later on when they show up, will tell you that the rate has increased significantly. So that's similar to what we were just talking about, but usually they won't pack your stuff up on the truck before you pay, so you know before your items are being held hostage that that's happening.

So that's something you want to keep an eye out for, and we'll talk about more red flags. But if you are out there getting quotes from three or four companies and one is significantly lower than the other three, there might be something going on there.

And then the other kind of scam that we see, and I would assume that this is probably the most common that occurs, is the no-show. You sign a contract, maybe you'll pay a deposit or a portion of the bill ahead of time, and then the mover just never shows up to move your stuff and they have your money— maybe it's a 50% deposit you put down. And then you're out of luck because you don't have any movers on the day that you need to move.

Watch out for these red flags

Devin: So those are the three outcomes that we see and there are red flags or things you should be aware of during the process, and steps you can take to ensure that you're hiring a legitimate company and not a fraudulent moving company.

So, the number one thing, like I was saying, is to beware of those suspicious quotes. So again, you should be inquiring with more than one company and then comparing those quotes. If three of them are in the ballpark, and then one is super low, you might think that there's probably hidden fees or

something going on with that company. You should probably suspect that you're going to pay more when they show up, or something else is going to happen.

There is actually a database for movers, a national database. It's called the Federal Motor Carrier Safety Administration. And all moving companies are supposed to be registered there. For the most part, I would recommend that people check there and only hire a company that is registered with that organization.

Obviously too, you want to look at Google reviews, Yelp reviews, to make sure that people have had good experiences. And if you have a neighborhood Facebook group or forum, going there and asking people's experiences can be a way to help you avoid falling victim to a scam. But I would start with making sure you're hiring a registered company because they have to follow certain rules.

Second, like I said, beware of those suspicious quotes where it's really low compared to others. And obviously, you want to read your contracts carefully before you sign them. Make sure that there's no kind of hidden fees in the fine print because that's where a lot of this will be. **Never sign a blank contract.**

You should ask for a certificate of insurance from the movers to protect your belongings, your home, where you're leaving, where you're going to. That's really important too. If they're unwilling to provide that, it might be a sign that there's something fishy going on. So you want to take those precautions.

What to do if you are defrauded

And if you do fall victim to moving fraud, there are some steps that you can take. You can file a complaint with that federal agency that I mentioned earlier, the Federal Motor Carrier Safety Administration. And then you can also file reports with the Better Business Bureau and the Federal Trade Commission.

Obviously, that's a headache, and having your items either missing or spending a lot more is a headache too. So look out for the kind of issues we talked about. Go with someone who's trusted in your area from word of mouth or online reviews. That's where you want to start because moving isn't fun to begin with. And if your stuff winds up sitting on a truck somewhere or never arriving, that makes it even worse.

New study on cyberattacks cites top 3 threats

Sean: Right. OK, so moving on. There's some new research out about how cyber attacks occur. Let's find out what that's about.

Devin: Yeah. There is a study out from Palo Alto Networks. They do a lot with security and cybersecurity. This study solidified some of the things we've been saying here in Hack Proof Your Life Now and the cybersecurity program for years: certain threats are really the ones that you have to be on the lookout for, they cause the majority of cyberattacks, the number one being ransomware.

We've been saying that for forever now.

Ransomware, that's when you're clicking on a malicious link, it downloads malware onto your computer and locks it up. All of your data's encrypted and you have to basically pay a ransom to get that money back if you don't have a backup. So that's one of the biggest threats we're seeing, as well as software vulnerability, which is running outdated software on your computer thus leaving it open for hackers to come in.

They said that software vulnerability accounts for nearly half of all cases of initial access. So that means that it accounted for half of the cases of hackers getting into corporate networks to then deploy ransomware.

So those two top threats, they're working in conjunction with one another. The outdated software is allowing the ransomware to be installed and work. So those are two principles we talk about in the book, keeping your software up to date always, and being on the lookout for ransomware.

And then the third biggest threat they talked about was business email compromise. We talk about that in our book, Hack-Proof, but also in the Savvy Cybersecurity for Business presentation. Business email compromise, for those listening who aren't familiar with it, is like a phishing email, but specific to a company. So a hacker will impersonate the CEO or CFO of a company, send something out to other employees who maybe are in control of wiring money or something to do with accounts, ask the employee to move that money, wire that money to this other account, and it winds up being not from the CEO or CFO. It's a hacker and the money is going to a bank account that does not belong to the company.

So this study came out and basically said these three are the top causes of cyberattacks that businesses are seeing.

Business email compromise a top threat

Sean: Right. And of course, the Savvy Cybersecurity program has a special presentation to deliver to business owners and people who are in management at whatever company they're working for, and talks about the business email compromise among other things. Yeah, that's a scary one.

We've seen it at work at Horsesmouth. The attempt was foiled, but people get inside your networks and start lurking, and then they start to pretend to be the CEO at the appropriate time, sending directions to financial, your CFO, or business manager, or whatever the case may be, people in accounts payable.

And some really terrible and disastrous things have happened because of the devious way that these hackers are working, lurking and understanding the patterns and the key people at play in a network. And then they strike when the CEO is in a meeting, or on a plane, or on vacation, or whatever the case may be, or late Friday afternoon. "We've got to rush this through." And all sorts of common sense is overridden by people suddenly being stressed out about needing to meet a deadline to get somebody some money, and disaster ensues.

So keep your software updated. Keep everybody aware of what ransomware is, and what the business email compromise is, which I believe, Devin, at times in the last few years, the FBI has listed the business email compromise as a top threat to companies. Right?

Devin: I think it's considered the number one threat to companies. And the FBI has released reports basically saying, "It's increasing every single year. We're getting more complaints every single year." Like you were saying, we've seen it here before.

I've spoken to other business owners who've seen it. I've gotten impersonated emails from other companies that we've worked with before, so it is affecting a lot of people, and it definitely is something that you want to be aware of.

Sean: Right. And of course, one of the simple solutions I think they recommend on the business email compromise is that no money is released. It's almost like a two-factor authentication, two different people within the organization have to sign off on it and it has to be done verbally.

Devin: Yeah. You want to confirm via phone, Zoom, face-to-face. You don't want to just be wiring money based on an email request.

Sean: Right, unless the email comes from me, then it's OK. All right. And then lastly, our friends over at T-Mobile have had some challenges recently. What's going on with them?

The T-Mobile settlement

Devin: So last year, T-Mobile had a huge data breach, basically exposing 70 million customers' information, birth dates, name, addresses, phone numbers, all of that. Now we're seeing the outcome from that—they have agreed to a $350 million settlement based on the data breach.

This will be the second largest data breach settlement following the Equifax breach in 2019, which was $700 million. So if you are a T-Mobile customer, you may be entitled to part of this settlement. It's probably only going to be $25 a person because so many people were impacted by it. But hey, if you are impacted, you should know about how to get that money. So T-Mobile will reach out to you if you were affected by it. And you may already know if you are, but you should still get communication about how you can file to be part of that settlement.

But this is a promising thing that we're seeing companies being charged this high amount of money for these breaches. I think probably the only way we're going to see companies start to take this a little bit more seriously is if they have to pay out these huge fees. So I think it's a positive thing that we're seeing such a large settlement because hopefully that means other companies will see this and start to take security a little bit more seriously. So if you are a T-Mobile customer, or you were last year, keep an eye out. You should receive something in the mail.

And this is a time for me to also remind people that when we see things like this, scammers take advantage of it as well. And you may get phishing emails saying, "Click here to get your money." Just keep in mind that T-Mobile has said official communication from them will come in the mail, hard copy. So if you get emails, or texts, or phone calls about it, do not click on any links. Don't provide any information. Look for the hard copy in the mail before you do anything.

Have a core defense

Sean: Right. And I guess with this T-Mobile breach, it's yet another chance to remind advisors that everybody's stuff is out there in the dark market. For a very small amount of effort, I could have Devin's date of birth and her social security number and everything else about her.

It's out there already, and that's why it's so important, as we say in our Savvy Cybersecurity Program, to have a core defense. We do preach a core defense that all your clients ought to have, including frozen credit reports. You want to do that. You want to have two-factor authentication on all of your email accounts, and also your main financial accounts. All that needs to have two-factor or multifactor authentication now because we're moving beyond just two-factor….

And then the third thing is notifications of when money's going out of your account. Right? And so if you have those three things in place, plus you're doing some of the other things we recommend like updating your software, that's a critical aspect as well, you have much better chances of remaining secure.

Clelan and Company, 210 Grandview Avenue, Suite 101, Camp Hill, PA 17011
www.clelan.com financialpro@clelan.com