Hadley

How to Avoid Phone and Online Scams When

Living with Vision Loss

Presented by Ricky Enger

**Ricky Enger:** Welcome to Hadley Presents. I'm your host, Ricky Enger, inviting you to sit back, relax, and enjoy a conversation with the experts. In this episode, we discuss tips and tricks for avoiding scams, and our guest is low vision blogger Veronica Lewis.

Welcome to the show, Veronica.

**Veronica Lewis:** Thank you so much for having me, Ricky. I'm so excited to be here.

**Ricky Enger:** It is delightful to have you. I've read your blog. Sometimes I read it on your website and sometimes I find the info elsewhere, so you do get reposted a lot, which is fantastic. For those who are not familiar, you have the site Veronica with Four Eyes. That's your blog. And we're going to talk about scams today. But before we do that, I'm wondering if you could just tell us a bit about yourself.

**Veronica Lewis:** Thank you so much for having me again. Yeah. My name is Veronica Lewis. I run the Low Vision Assistive Technology website, Veronica with Four Eyes, where I help people with visual impairments learn to thrive both inside and outside of the classroom, workplace and in their living environments. I started Veronica with Four Eyes back in 2016 because I noticed there weren’t a whole lot of resources out there, specifically targeted at living with visual impairment, and I wanted to share the things I had learned with others as well. My website can be found at V-E-R-O-N-I-I-I-I-C-A.com, so that's Veronica spelled with four I's.

**Ricky Enger:** Love it, and we will have a link to that in the show notes. So if you're frantically writing and didn't quite get that, no worries, we'll have that for you and it's well worth the read.

As I mentioned, we are going to be talking about scams today. Certainly not everyone's favorite subject, but a necessary one. I think any general info about scams is a good thing. So, if you're watching maybe the local news and there's a segment about scams or maybe you're reading something in a newsletter, that info is always great. But I'm wondering, for our discussion, are some characteristics that may make us a little more vulnerable to scams because of some aspects of our vision loss?

**Veronica Lewis:** Absolutely. One that comes to mind is that people may have trouble reading things very carefully or picking up on differences with formatting or spelling. So for example, a lot of scam emails come from what looks like a real company, but maybe one or two letters have changed or maybe the font has changed, so the logo looks different, and these may not be details that people would pick up on. I know I get a lot of emails of that nature where it will claim to be from PayPal or from all of these different social media sites or websites, it'll have the name of the company in it but can even just have different phrases and weird things in there. But if you're looking at something non-visually or reading through a screen reader, you may not immediately pick up on these things.

Another thing that also comes to mind is I feel like a lot of people will share a lot of personally identifiable information online, especially when they're new to living with visual impairment and are just desperate for resources. I get messages from people sometimes where they will include their full name, the city and state they live in, their diagnosis and even things like their phone number and address. I am always surprised when those come through because you have no idea where that email's going or who could actually be receiving it. I think the nature of oversharing in an attempt to find resources can also make people particularly vulnerable to scams because you can sometimes track down someone with a visual impairment with these two pieces of personally identifiable information. Even a first name and a diagnosis can sometimes be enough to find a lot of information about somebody and having that information in so many places online can definitely make people more vulnerable to scams in that regard.

**Ricky Enger:** Yeah, that makes sense and it's actually a little bit terrifying if you think about it. It's no wonder that I hear people say, "I just want to avoid all of this. I'm not going to mess around with any of this online stuff. It's just too much. I'm going to stay safe just with my phone. Maybe I'll do a little texting or whatever, but not going online to where the scams are." But the truth is the scams are everywhere. They happen on the phone and text too. So maybe let's talk about that. What are some scams that can happen, maybe by phone or by text?

**Veronica Lewis:** I know one thing that comes to mind is a lot of text alerts for fake two-factor authentication codes for logging into a website or people may be prompted to give login information through unencrypted text or things like that. Another example that came to mind as well was just spam phone calls. You have no idea how many calls I've gotten from my car's extended warranty, and I've never operated a motor vehicle. It's been pretty bananas just to see how many spam calls and texts people can get in a single day and how many of them can look realistic and something that people need to respond to. I feel like a lot of these scammers have become skilled at sending messages or phone calls that generate anxiety or fear and make people feel like they have to reply right away. So learning to spot those tactics can help to protect people as well.

**Ricky Enger:** That's a really good point. There is a staff member at Hadley, Lisa, she tells the story of her dad getting a call and the caller on the other end says, "Devin is in jail," and this is his grandson, "and we need you to respond immediately. I'm the police officer. You do need to pay in order to get him out of jail," and all of that. So it's a huge adrenaline spike. Right? Well, fortunately Devin just happened to be visiting her dad, so he was right there in the room. That scam didn't go so far. But what happens if you don't have your grandson right in the room and you get a call like this saying you have to respond now or else kind of things? How do you deal with that?

**Veronica Lewis:** I think it helps to know how these processes actually work and know that there will never be a situation where you'll have to wire money over the phone to get somebody out of jail. That's not a thing that happens. Another thing that stood out from that story though is how did they know her grandson's name, Devin? Where did that information come from? So it can also be if you have Facebook, just locking down privacy settings, so not just anybody can just find out that information or find out all of these other names as well.

One of the things that can help with the adrenaline rush situations is also knowing how to contact the real business or the real agency that gave you a call to begin with. Let's say the grandson's in jail, know that you can hang up with this person and then call back the jail and talk to somebody else. In that real situation, they'll understand that you want to verify things and make sure things are the way that you say they are. I think it's also important, with some of these scams to know that they will say, "Hey, I can call you back and you'll see on my caller ID that I really am with this agency," but the thing is that they can spoof the caller ID, they could spoof a phone number. It's no grand accomplishment that they were able to call you back with the phone number that they say on the other organization's website. It's important to take the time to make those calls for yourself and just make sure you're doing your research that this organization is who they say they are.

**Ricky Enger:** Yeah, and it sounds like really what you're talking about is the overall feeling is to take that step back and let the logic come into play, so don't respond immediately. Have that time to do the research to make the call back, don't react to what's happening, take that step back so that you're absolutely sure about what's happening.

I'm wondering also about if you're planning ahead, are there things like talking with family members and having maybe a code word in place or something that if you needed to verify it was definitely your family member? You've talked about it over beforehand about what to do in this situation. Have you heard of people doing this?

**Veronica Lewis:** Absolutely, and it's something I have with my family and my friends as well. Everybody has their own special word where I can verify it. And another thing too is I've made it a word or an interest or something that that we don't talk about on social media or on public platforms. So somebody else wouldn't be able to say like, "Oh, I'm pretending to be this friend. I saw your post at one point about how much maybe you love this certain activity, so I'm going to say a word that's associated with that activity, so you know it's maybe associated with this person." So I think that's really valuable, just keeping that information safe and making sure that no one else would be able to guess what the word is.

Another thing also, I know some people answer a question that I think only this other person could figure out, but again, with all the publicly identifiable information online, you have to really make sure it's a strong question and not something like a security question about who's my favorite teacher? Where did I go to high school? Because I'm sure people could go back and find that.

**Ricky Enger:** Yes, indeed. These are some good plans to have in place if something like this should happen. Are there any tools for stopping these phone or text scams before they happen, like maybe a tool from your phone provider or talking caller ID, things like that that people might use just to be aware of what's happening before they even pick up the phone or look at that text?

**Veronica Lewis:** Absolutely. A lot of companies like Apple and Google have also created their own tools for iOS and Android respectively for screening scam calls and numbers having them just go straight to voicemail or disconnect. The block tool is a really great thing to have. There are also tools that will let you block an entire area code if you're repeatedly getting spam calls from a specific area code that maybe doesn't even exist in the United States.

Another thing that came to mind as well is there's a spam and blocked option for messaging apps a lot of times. They'll filter through messages that seem to be a scam or associated with scam numbers, and those tools seem to work really well. There’re also third-party apps as well that can provide more enhanced caller ID and protection features as well, and they also may provide more options for blocking as well.

**Ricky Enger:** That makes sense. We've talked about some offline scams, and sadly there are a lot of them. For people who do choose to go online, whether it's for shopping or social media or email, all of these things are wonderful, wonderful tools, but they also leave us vulnerable to scams. So what are some of these common scams that people might find online?

**Veronica Lewis:** Oh, a lot of scams come to mind, unfortunately.

**Ricky Enger:** Yeah, no doubt.

**Veronica Lewis:** I've seen a few things for fake job listings, fake products that are being offered through Medicare or Medicaid, especially assistive technology products if you're online shopping, sometimes. This is kind of funny actually. I get receipts from fake companies for things I did not order. One of the examples I share on my website actually is I had gotten a fake order invoice that said, "We charged this to your PayPal.” This receipt has your name and an address on it, but I think it was for a 15-foot-tall inflatable water slide for the backyard. And they said, "If you didn't order this, please call us with your PayPal number." And it's like, no, I'm not doing that. And besides, I knew that the address they had shared, the email and all these other things were definitely fake.

Another scam also that comes to mind, which isn't necessarily the traditional thing you think of when it comes to a scam, but it's related to sharing images and things online. I've seen some accounts on social media will put in fake or misleading alt text for images to get people to tweet them or reshare them or whatever on their profile. So they'll think they're sharing a picture of one thing, but it's actually something much different.

**Ricky Enger:** Oh, yes, right. This is a good one! So if you have enough vision where you’re able to discern images pretty clearly, this is probably not going to apply to you. But if you’re having the text on your screen read aloud so if you’re using a screen reader, this is definitely a thing that could happen.

So when you encounter graphics or images, they might say “graphic” or “image” or “blank” or whatever because someone has not bothered to describe that image. But if someone does add a description, that is “alt text.”

So what you might have is something like a picture of a black dog playing in the snow. And someone adds a description to that image so that your screen reader says, “black dog playing in the snow.” I guess what’s happening here though, is that the description does not match the image. So you may think you’re sharing that picture of a black dog playing in the snow but maybe not so much.

**Veronica Lewis:** I actually had this has happened to a few of my friends unfortunately, where one of them had reposted a picture. I think it was on Twitter at the time, and when I looked at the alt text, it said it was a picture of a sunset with an inspirational quote, but the actual picture was something very much different. It was actually something that was explicit. So I ended up calling my friend on the phone and saying, "Hey, did you mean to share this? Do you know what's in that picture?" And they were mortified because they had no idea. One of the posts I have on my website is about how to access images without alt text. And it's important when you're on social media sometimes where if you're resharing something from an account you don't know, maybe it showed up in your feed through the algorithm or whatever, it can be helpful to just run the picture through a visual assistance app to make sure it is what you think it is.

**Ricky Enger:** Yeah, that makes perfect sense. If you're not able to see that image, be careful about what the alt text description is telling you it is. Sometimes even if you can see the image, there will be things that happen where on social media you might see a picture of someone and it says, "Oh, I'm going to miss him so much," and the implication is that the person has passed away and there's a link that you can click to learn more information or read the obituary or what have you, and the link for that is the scam. And when you click that, goodness knows where you go.

So again, it sounds like what we're really talking about is while we're sharing some specific scams that people might run into, the general thing to do is to carefully look at whatever it is you're doing before proceeding. Whether that means if you're using a screen reader, you're spelling things letter by letter, or if you're reading it visually, that even though you've got that eye strain, it can be important to just take the time to carefully look at those things to make sure that it's what you thought it was at first glance. Right?

**Veronica Lewis:** Absolutely. Another strategy that came to mind as well for helping with email scams is I take the trusted domains for websites. For example, I need notifications from WordPress for my website, I white listed the WordPress email extension so I know that any email that comes from there is likely from WordPress, and I filter those to a folder in my email so I know that when I open that folder, it's actual emails from WordPress as opposed to the scam emails pretending to be WordPress that may show up elsewhere.

**Ricky Enger:** That's a really good idea to do some of that filtering beforehand. And if you're thinking, "I have no idea how to do that," we're happy at Hadley to direct you to some of these resources for just the technical part of doing that. We can be as careful as possible and try and think through all of these and say, "Okay, I've got a plan in place and so on," but sometimes the worst happens anyway, and we find that we have been the victim of a scam. So if that does come to pass, are there some tricks for just navigating that and getting safely on the other side?

**Veronica Lewis:** Absolutely. One of the things that comes to mind is that when it comes to changing passwords, the first one you should change is your email password, because if somebody has your email password, they can hit the forgot password button on any other website and change all of the passwords for you, and then it'll be much harder for you to get them back. It's very important to make sure if you have a compromised account or anything was compromised, definitely secure your email first and then work on securing everything else.

Another thing is just being honest about what happened and reaching out to family members or other groups for help and saying, "Yes, I know I got scammed," instead of keeping it secret because you can't believe it happened to you. Be honest about it and let people help you try to get everything fixed again. I think that's really important as well.

Again, being on top of things like making sure that your bank account is secured, changing the passwords there, of course, freeze the cards if needed and make sure that when you are contacting places to help with this that you are using their official phone numbers that you find directly on their websites, not something you may have found in the recommended first result on a search engine. Sometimes scammers will pay to have those phone numbers listed first.

I had an issue at one point where I was trying to find a hotel reservation and I thought I had booked something over the phone. Luckily, I did not give any credit card information. I had just given the information over the phone to book a hotel, and when I went there the next day, I found out I had never actually made a reservation. So that was really frustrating, but I was able to get it fixed. I felt very silly because I couldn't believe that I had fallen for that scam, but it turned out that the phone number I had called, I had asked the Google Assistant to dial this hotel chain, that phone number was the first in results, and that's what came up. That was many years ago. Luckily, that issue has been fixed, but that was another thing that came to mind, sometimes these fake phone numbers can take precedence in the search results.

Another tip I had as well was to save the accessibility support phone numbers for tech companies and things like that. These are specialty phone numbers that are designed to support assistive technology users, such as people who use screen readers or screen magnification with being able to access their products. There's a lot of different companies that have these, Amazon, Microsoft, Google, and telecommunications companies. Those are another helpful thing to contact if you're having trouble with accessing a product or accessing a billing service.

**Ricky Enger:** Yeah. Those are all really, really great points. I especially appreciate when you said to be honest about what happened, because I do feel like there is some shame around, "Oh, I got taken. I fell for this." People are reluctant to admit that, but the truth is that it can happen to anyone, and it doesn't do you any good to hide that. It's okay to admit that moment of vulnerability so that you can move forward and get things fixed.

This has been amazing and just a wealth of information. We'll have a lot in the show notes and direct you to some resources.

These are all really, really great tips. It may sound a bit overwhelming at first like. I have to think about all of this before I even do anything, but once we break it down and say, what you're really talking about is just taking that extra second or two to think through what you're doing and then deciding to proceed. Once you have all the info you feel like you need, that can be a wonderful thing. And having those plans in place if something unexpected does happen, you kind of know what to do next instead of reacting with that adrenaline and thinking, “Oh no, I have to get this fixed or I have to respond immediately.”

So thank you again Veronica so much. This has been fantastic and informative, and I am so glad you took a little time to join us.

**Veronica Lewis:** Thank you for having me.

**Ricky Enger:** Got something to say? Share your thoughts about this episode of Hadley Presents or make suggestions for future episodes. We'd love to hear from you. Send us an email at podcast@hadleyhelps.org. That's P-O-D-C-A-S-T at hadleyhelps.O-R-G or leave us a message at 847-784-2870. Thanks for listening.