The Collector Chronicle

North American Recovery | January 2022 | America's Collection Authority

Last Month's Lucky Winner

The winner of our client prize for December is Mountain Valley Eye Institute. They've been using our agency for over nine years. We'll be sending them a gift basket from the Chocolate Covered Wagon. Enjoy!

This Month's Prize

This month we will be giving away a gift basket from the Chocolate Covered Wagon. Each client who sends new accounts during the month of January will have their name entered into a drawing. At the end of the month we'll draw a name, and if it's yours, you'll win the gift card!

Don't miss out on your chance to win!
Send us new accounts before the end of the month!
Good luck!!

CHOCOLATE COVERED WAGON

Spotting Red Flags in Emails

By David J. Saxton
President, North American Recovery

There's an old phrase that says, "A sucker is born every minute." Ironically, that was said by a man who bought a fake fossil for his art gallery after being scammed into believing it was real. Although most of us probably don't have to worry about scammers selling us fake fossils, there are still plenty of ways those nefarious ne'er-do-wells will try to pilfer your purses for every penny they can plunder. In this month's newsletter, I wanted to share one example of the most common email scam I know of, as well as one example of the diligence of our employees.

First, let's start off with the email scam. One of the most common things scammers will try when perpetrating their misdeeds is attempting to impersonate a legitimate business when asking for information. The easiest way for them to do that is to use a small detail that very few people ever take into consideration: text fonts.

The vast majority of default text fonts for email apps and web browsers are what's called a "sans-serif" font. This means, among other things, that a capital "I" (9th letter of the alphabet) and a lowercase "L" (12th letter of the alphabet) will look exactly the same to most people. To demonstrate, here's an example of several "L's" and "I's" in a sans-serif font:

lllllllllllllllllllllllllllllllllllllllll

It's a mess, right? It just looks like a barcode, but I can assure you that not all of those letters are the same. But how can scammers exploit that? Well, they do that by creating fake email addresses that look real and are attempting to impersonate a real business.

For example, let's say you just got an email from Intermountain Healthcare. It looks completely official and comes from an email address called "Finances@lntermountainhealthcare.org." Looks legitimate, right? Unfortunately, it isn't. Let's look at it again, but this time, everything will be a capital letter. This makes the problem very easy to spot.

FINANCES@LNTERMOUNTAINHEALTHCARE.ORG

The Collector Chronicle

North American Recovery | January 2022 | America's Collection Authority

See what I mean? So how can you avoid these types of scams? Well, the vast majority of the time, there will be one or more red flags in the email that should alert you to the email's dubious nature. These are things like misspellings, bad grammar, not having a signature at the bottom, or certain businesses asking for information they should already have. For example, this sample message has A LOT of red flags in it:

Dear Mr or Ms Doe,

This is official correspondence from the finance department at Intermountain healthcare. Your account with us has become delinquent and is in collections unless you pay in full immediately. It is in you bset interest to pay this immediately at our website lntermountainhealthcare.org. If you do not do this immediately your account will be in collections.

regards,

finance department

Can you spot all the red flags? I count eight. The big one I want to focus on is that "website" they're peddling. It's nearly impossible to tell because of that email's font, but it has the exact same problem of the example email address I showed you on the first page. The "I" at the beginning is actually just a lowercase "L."

Luckily, there are a couple of very easy ways to tell if that "website" is legitimate. Firstly, don't follow the link. At best, it will lead you to a website that LOOKS exactly like the real thing, but it's just a façade designed to get your payment information as quickly as possible. What you can do, and should do if you're suspicious, is copy the plain text of the email and paste it into your favorite word processor. Again, be careful not to follow any links or download any attachments. Back in the word processor, you can change the font to your heart's content. By changing the font to Times New Roman, a font that doesn't have the same problem as the default font of most email applications, you'll quickly see that the website is actually called lntermountainhealthcare.org and not Intermountainhealthcare.org like it should be. If you're still having some trouble spotting the difference between the two, you still have another option. You can copy that same plain text into a text-to-speech program or website, such as Google translate, and click on whatever option would read the text aloud. The computer will know the difference between an "L" and an "I" regardless of what font is used. This means that when the program reads the word aloud to you, it will sound wrong. After all, Lntermountain isn't an actual word.

I also wanted to share with you an example of our employees' diligence at preventing scam emails from harming our company. Although it turned out to be a legitimate email, it was constructed in a way that made it appear very suspicious. First, the signature was plain text with no logo. The email address was very generic and initially unfamiliar. On top of all that, the entire message was contained in one line with next to no punctuation. On their own, all these things should be setting off warning bells, but when this many red flags are combined, that's when there's a problem on your hands.

This email eventually got forwarded to Lisa, our Vice President of Operations. She immediately recognized the email address even with the limited contact information available. Still, she played it safe and called the law firm to confirm the legitimacy of the email. Even though she knew the law firm, the email wasn't formatted in the usual way and the two attachments had names that were vague, giving no indication about what was contained within them. Once she called and confirmed that the email was legitimate, she was able to carry on with her job as normal knowing that our internal network wouldn't be at risk.

So that's really the big takeaway from this newsletter. Scammers rely on you to be unalert and undereducated in order to do the things they do. Hopefully this newsletter has provided something new that will help you avoid getting scammed in the future. Thanks for reading, and thanks for sticking with NAR.

NAR
North American Recovery
Professional Debt Collection Services

The Collector Chronicle **is published monthly by North American Recovery for prospective and current clients. Please direct questions or comments to the editor, Dave Saxton at DaveSaxton@North-American-Recovery.com**

1600 West 2200 South, Suite 410, West valley City, Utah 84119 • 801-346-0777
www.North-American-Recovery.com