SPOTTING AND DEALING WITH SCAMMERS

PHIL RICE

Spotting and Dealing with Scammers

By Phil Rice
Owner, PRR Computers LLC

www.prrcomputers.com

September 2022 Edition

Introduction

Scams are nothing new. There are certain types of people who have been out to swindle other people out of their money since, well, since before money was even a thing!

You might think scams are on the rise recently, what with all the technology now at criminals' disposal.

And you'd be right.

Every day, thousands and thousands of people are bombarded by attempts at deception – on the phone (sometimes by humans, sometimes by robot callers), by text message, by email message, by voicemail message, by website pop-up message…

There is really only one defense against this barrage:

A little education.

Types of Scams

Here are some of the types of scams you may spot “in the wild” on your various devices:

Fake Tech Support

These typically begin with a scary looking (but 100% fake) security warning message on your computer screen, claiming your computer is infected or hacked. Inevitably there’s some kind of toll-free phone number you are urged to call so a technician can fix this for you. Often they will claim to officially represent Microsoft or another company name you might recognize.

Do not believe it!

These phone numbers connect to call centers – typically overseas – filled with agents who are trained to trick you into giving them remote control of your computer, and then that leads to any number of schemes designed to get you to fork over money for illegitimate reasons.

DO NOT CALL. And never, ever give remote access of your computer to someone you do not know personally.

Amazon Account Problem

This one is growing in popularity recently; a “customer service representative” from Amazon or another online shopping vendor reaches out to you and says your account has been used to make a big purchase, or that someone has stolen your identity to make a big purchase… and they offer to fix this problem for you.

DO NOT BELIEVE IT.

Hang up, and do not give them any information. It is all a scam to deprive you of money through an elaborate scheme which talks of “refunds” and such – it is all a ploy.

Roku “Expiration”

This is another relatively recent scam, targeting owners of Roku streaming devices. A representative will inform you that your Roku software has “expired” and you need to renew it to continue using the device.

IT’S A LIE.

Roku devices may get old over time, but the software does not expire. And Roku does not even sell the “service package” these scammers are trying to trick you into buying.

Refund Scams

Perhaps the trickiest and most enticing of all scams, this one is where a supposed representative of some company contacts you to say they owe YOU money for some reason and want to get the money back to you.

THEY ARE LYING.

The way this scam works is somewhat fascinating, but highly dangerous. Search YouTube for videos about “refund scams” to see how they work.

What is important for now, though, is just to understand that while on the surface this scammer will appear to want to send money to you, they will in fact turn the tables and money will only go in one direction – from you to them.

IRS / SSA

Some scam outfits specialize in posing as the Internal Revenue Service or the Social Security Administration in this frightening extortion scheme designed to scare you into paying money under threat of arrest, freezing your bank accounts, etc.

IT’S A RUSE.

Check out this video where a well-known “scam-baiter” exposes the IRS scam:

https://bit.ly/irsscamexposed

Loved One In Trouble

This scam sometimes pretends to come from a lawyer or a doctor representing the interests of a real person you care about who is in legal or medical trouble – asking you for money to help them for some emergency. Sometimes the contact appears to come from the real person themselves, made possible from a compromised email account for example.

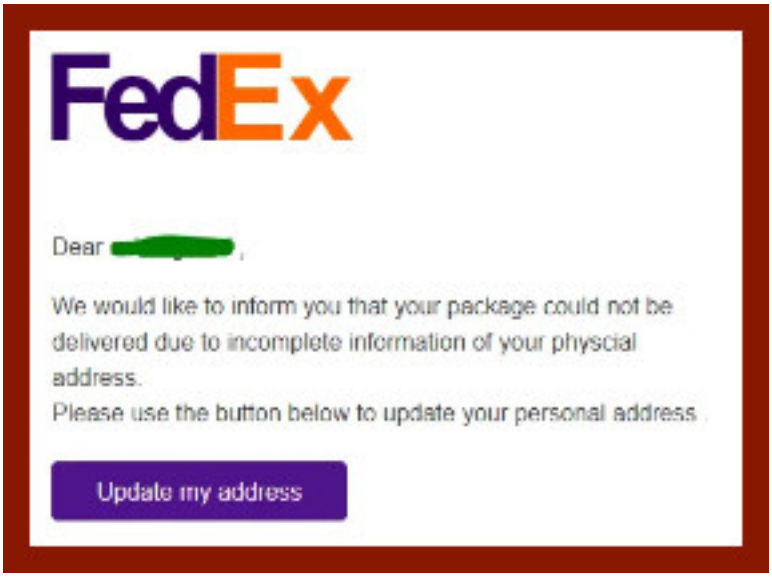
IT IS A SCAM.

If you are approached in this way, stop the communication, and directly call the real person you know. This will make clear that someone was trying to fool you and will put your mind at ease about your loved one.

Fake Package Info

An email or text arrives, often looking very official, with a link you are supposed to visit to check the tracking info on a package.

BE VERY CAREFUL.



These communications can be easily spoofed, with a fake link taking you to a fake website designed to steal a username and password from you. These are particularly dangerous because as we all know, sometimes indeed we are looking for a real notification to come about a real package. The scammers are counting on this and are hoping you will let your guard down.

Most legitimate notifications (text or email) from package delivery companies have the information you need right there in the text or email, and do not require you to visit a link or login to anything.

Fake Bank or PayPal Notice

An email or text arrives, with some urgent information from your bank or perhaps from PayPal. These are cleverly designed to look authentic and are almost always paired with a fake website designed to steal your sign-in information.

NEVER TRUST THESE EMAILS.

First, no legitimate financial institution uses email to contact customers about urgent issues. Not at all.

Secondly, if one of these messages raises questions for you, do NOT use the link they provide in their email or text. Instead go to your web browser or app and visit your financial institution in the normal way you do. Then you can check on your accounts to

put your mind at ease. Of course, call the financial institution (using the phone number on their real website) if you see anything that is cause for concern.

Fake Document Sharing Link

Scammers like to send emails with links to “important” documents which they are delivering to you via Microsoft OneDrive, Dropbox, or some other secure file sharing service.

DO NOT TRUST THESE INVITATIONS.

If you are not explicitly expecting to receive a document from that specific person, then do not click the link. Instead, contact that person (by phone, if possible) to ask them whether they are actually sending you a file.

It is highly recommended NOT to reply to the email message to ask this question, because it is very possible that the reply will go to the scammer who is pretending to be your colleague so they can continue their deceit.

There are numerous other types of scams, most of which fall under the categories of either “too good to be true” (someone wants to give you a large sum of money, or you’ve won some sort of prize or gift) or “intimidating” (your student loan lender is preparing to sue you).

The many communication options we have in this world provide us with some conveniences that would sound like far-fetched science fiction to people from fifty years ago… but with that convenience comes dangers like the above. So, it is important to always stay vigilant.

With such a variety of ever-evolving scams, are there some general rules for spotting them?

And what do I do if I find myself caught up in a scam?

I am so glad you asked!

Read on for further info.

Telltale Signs

Most scammers are after your money, and unsurprisingly, most of them do not say so up front. Instead, they are hoping to manipulate you into certain actions that may seem okay, under the premise that they are here to "help" you. Often you will find they are asking for things like:

- Remote access to your computer
- Asking you to sign in to your online banking (often while they are remotely connected to you)
- Asking you to go to a store and purchase gift cards
- Asking you for personal information over the phone, such as your address, social security number, your place of employment, the names and ages of your relatives or dependents

If you are asked for any of the above from someone you do not know personally, then you are almost certainly in contact with a scammer.

So now what?

What To Do

STOP!

If you are on the phone with someone you suspect is a scammer, end the call immediately. If they call back, do not answer. Additionally:

- Disconnect from the Internet. The easiest way to accomplish this is to unplug your router/modem.
- Turn off your computer. If you must, forcibly shut it down by pressing and holding the power button.
- Block the scammer's phone number on your phone, so they cannot call you back.
- If you have any reason to believe your banking or credit card information was compromised, call your bank immediately and notify them of the situation. They will have procedures for you they will recommend.
- In certain circumstances, you may want to involve law enforcement. If you believe your bank account or credit card was used fraudulently, or if you were threatened in a way you find to be credible, calling the local authorities is a good idea.
- Notify us at PRR Computers if your computer, email, etc. was remotely accessed in any way by the scammer. 239-244-1579. We will help you make sure the scammer has no continued access, and we will make sure they have not left behind any viruses or malicious software.

Preventive Care

So now you know what kinds of scams are out there, and you know what to do if you fall victim. But is there anything else you can do to help reduce the risk of falling prey in the first place?

- **HOME USERS** – While antivirus and other security software is a vital part of protecting yourself, the most valuable asset in defeating a scammer is having someone trustworthy you can contact any time to ask questions about a situation you may be facing. That is where our **PRR HomeGuard** program is a great value – year-round security, maintenance, and consulting for your home PCs or Macs, from a family-owned resource you can trust.

- **BUSINESS USERS** – Again, antivirus and firewall are important against these threats, but a knowledgeable team you can rely upon is even more important. A **Managed Services Program** with PRR Computers covers all your computer and network maintenance and security round the clock, with our knowledgeable IT consultants ready to answer your questions about suspicious emails, texts, or phone calls any time. Educating your workforce with some **Security Awareness Training** is an excellent way to make sure not just your computers, but the people who are using them, are part of your defense plan.

Resources

Password Manager (Home):	bit.ly/PRRpassmanager
Secure Password Generator:	bit.ly/PRRpassgenerator
Antivirus:	bit.ly/PRRantivirus
StopDat (free popup unlocker):	prrcomputers.com/stopdat
Online Backup for Home Users:	bit.ly/PRRbackup
Parental Controls Software:	bit.ly/PRRcontrols
PRR HomeGuard:	PRRhomeguard.com
Fun Computer Tutorial Videos:	bit.ly/PhilRiceChannel

Conclusion

I hope this eBook has helped improve your awareness of scams and threats out there right now.

The criminals behind these schemes are working every single day to try to get better at deceiving you.

I encourage you to align yourself with allies who are committed every single day to helping you keep these kinds of threats at bay so you can thrive in your pursuits.

If my company, PRR Computers, can be that trusted ally for you, great! Let's talk.

Phil Rice
Owner, PRR Computers, LLC

(239) 244-1579

phil@prrcomputers.com