Scams, Scams, Scams

Perhaps you are familiar with Warren Buffett's two most important rules of investing:

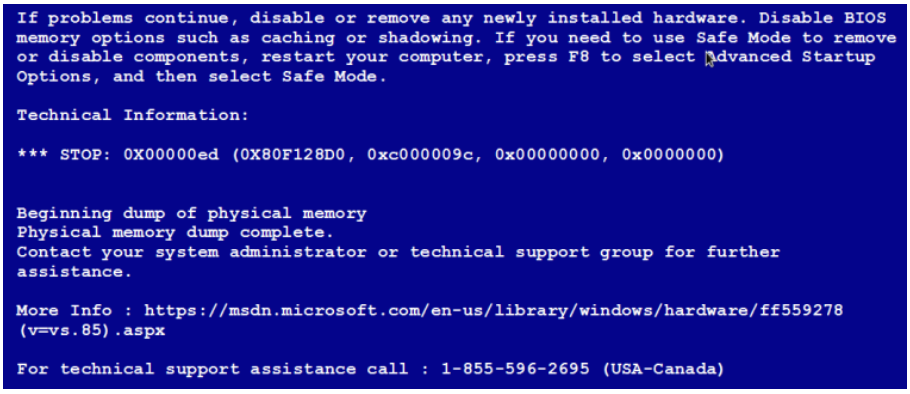
1. Don't lose money.

2. Never forget rule #1.

Today we're going to focus our attention on one sure-fire way to avoid losing money.

Blue Screen of Death

Have you ever been working on your computer, minding your own business, surfing along, and then all of a sudden your machine freezes up and confronts you with the dreaded "blue screen of death"? It would look something like this:



source: Malware Bytes

The image shown above is not an actual Blue Screen Of Death message from Microsoft, but it is a clever imitation designed by some nefarious souls as their initial overture into scamming you. If a person were to call the "technical support" phone number listed at the bottom of the image (tip: DO NOT CALL THIS NUMBER!!!!!!), the scammer that picks up the call will pretend to be a Microsoft support agent and will pretend to help you fix your problem.

What this "support agent" is actually doing is one of two things: (1) extracting your credit card information from you, so that they can take some of your money (usually a nominal sum of around $100), and/or (2) installing malicious software (a.k.a. malware) onto your computer which could do you further harm by tracking your keystrokes and thereby learning valuable information about you such as your social security number, passwords, and so on.

Other Scams to Watch Out For

Another scary ploy involves a simple piece of hardware that the criminal installs on top of a place where people often swipe their credit, debit, or ATM cards. The most popular places for these devices are on gas pumps and ATMs. Here, see if you can tell which of the following photos has an actual ATM card slot and which one has a "card skimmer" attached on top of it:

source: Krebs On Security

The ATM on the right has a plastic device installed on top of the slot into which you would insert your card. This device has in it some circuitry that will read the information embedded on the magnetic strip on the back of your card and a pinhole camera that will record your fingers as you type in your PIN code. When the scammer then comes to collect his hardware, he can use that information to print new cards which he will then use to make withdrawals from his preys' bank accounts.

Another scam involves the IRS. Anyone who knows your social security number and address can file a tax return on your behalf. Early in the calendar year, some scammers could fill out a bogus 1040 using *your* personal contact information but *their* bank account information, massage the numbers such that the IRS owes "you" a small-ish refund (usually a few thousand dollars), file it with the IRS, and then collect the refund (which the IRS usually pays out immediately before taking the time to inspect the accuracy of the 1040). Later, when you go to file your 1040, the IRS may be confused because it thinks you have already filed for that year. By then, though, the IRS' money—and the scammers who took it—are long gone.

Though we could go on with many more examples, we'll leave you with just one more important one. We have occasionally seen advertisements which prey on people's inherent fears. Given the underlying demographics, these typically air on conservative TV and radio stations. One we saw earlier this year urged its readers to: "Discover an asset class the likes of 'Rich Dad, Poor Dad' author Robert Kiyosaki, billionaire Carl Icahn, and President Donald J. Trump, have indorsed *(sic)* and/or invested in." These ads can involve exotic activities like buying "rare" gold coins or investing in complicated securities based on tax liens, or things as prosaic as variable annuities.

The one thing these ads have in common, though, is that they are nearly always promoting hucksters trying to separate you from your money, whether that's through the high fees charged by the security they're selling, or simple out-and-out fraud.

Remedies If You Have Fallen Prey

Up until now we've merely described some of the scams lurking out there, but now let's turn our attention to two important points: (1) what to do if you have fallen prey to a scam, and (2) precautions to take to avoid any future scams.

Let's talk first about the remedies to take if you have become a victim of one of these terrible things.

The first and most important thing to do if you have fallen prey to a scam is: don't be embarrassed. We are all human, and we all make mistakes. People from all walks of life have been taken advantage of, no matter how big their bank account or how high their IQ. It can happen to the best of us. So if you discover it has happened to you, it's best to just own up to it so that you can admit it to the appropriate authorities who can help you disentangle yourself from the situation.

If you believe your financial information (e.g., bank account number, investment account login, credit card data) has been compromised, immediately alert each involved institution. They may encourage you to open new accounts, transfer your assets into the new accounts, and close out the old accounts. They may also help you to recover any lost assets, whether through their own fraud protection systems or through filing insurance claims.

If you have purchased a sham investment, contact a trustworthy investment professional—preferably one with a fiduciary obligation to his or her clients—to help you figure out how soon you can get out of it without incurring too much of a loss.

If you have called the fake Microsoft support line or something similar, first contact a trusted source who is a computer expert. They can detect whether any malware has been installed on your machine and help you to scrub away any unwanted stuff while trying to retain your valuable files. Also, don't forget to contact your credit card company to file a fraud report, cancel your old card, and get a new one issued.

Precautions To Take

Now let's talk about what you can do to avoid these terrible scams in the first place. Here are some tips.

Change your passwords regularly. This goes for your email account, bank account, credit card, investment account, and anything else important.

Store your passwords in a safe, accessible place. Keeping them in a spreadsheet on your computer's hard drive is *not* advisable, because anyone who is able to access your hard drive will then have all your passwords. Ditto for writing them down on a piece of paper kept near your computer.

Even better than changing your passwords is to set up something called two-factor authentication. This is available for many email accounts, and it should be an available service from your bank or investment firm. In a two-factor authentication, the first factor is your password, and the second factor is a unique code that only you have access to. This code can be delivered to you either via a key fob which you can attach to your keychain, an app on your smartphone, or a text message delivered to you at the time you log in. The beauty of this system is that it regenerates a new random 6-digit code every 30 seconds or so. Anyone attempting to log in to your account who does not have both your password **and** your two-factor code will be locked out.

Use caution when taking money out of an ATM: cover the keypad when typing in your PIN and give the card feeder mechanism a good tug before inserting your card. Also keep in mind that it's far more likely that you'll be mugged at an ATM than have your card info stolen, so make sure you are in a well-lit place with easy egress to safety. Also, it would be wise to keep your checking account balance as low as possible, so that if your ATM card info is indeed stolen, the thieves will have access to a relatively small account from which to plunder.

Periodically check your credit report. The Federal Trade Commission has a program in which you can access your credit report for free once each year. You can either visit the website at www.annualcreditreport.com or call the FTC at 877-322-8228. There are also credit monitoring services for which you can sign up. For a fee, these companies will keep an eye on things and immediately notify you if something credit-related happens, such as a new account being opened in your name. There are many services like these, but some of the larger ones are LifeLock, Kroll, or TrustedID.

Consider anything abnormal to be a threat. When it comes to people trying to access your money or passwords, sign a contract, or otherwise gain access to your sensitive information, flip the U.S. justice system on its head: consider them "guilty until proven innocent."

And finally, if you do happen to watch conservative TV or listen to conservative radio, please tune out the investment-related ads.

Conclusion

While we have talked about a few scary scams today, keep in mind that there are many more scams out there besides these: dozens, maybe hundreds.

But remember: don't be embarrassed if you get hit by one. It can happen to the best of us.

And if you do get hit, it's not the end of the world. Sure, it will be a huge hassle to change all your passwords, cancel and re-issue your credit cards, and possibly change your bank account numbers, but … it's only a hassle. Life goes on.

The FDIC will be there to protect your bank accounts (up to $250,000 each), and SIPC will be there to protect your investment accounts (up to $500,000). Don't allow that protection to let you become complacent, but there's also no need to become obsessed about it.

Try to land in a happy middle ground: be wary but not vigilant. After all, life was made for living, so get out there and have fun and enjoy the many, many good parts of the world.

Felipe Garcia, CFA
Chief Investment Officer
INKWELL CAPITAL LLC

Aaron Byrd, CFA
President
INKWELL CAPITAL LLC