Congratulations! You've Been Scammed

Congratulations! You have been selected to receive a very special offer. We have heard that you or someone in your household enjoys traveling. We're actually looking for a few people willing to occupy unused cabin space aboard a magnificent cruise liner for free. We give you a free Bahamas luxury cruise simply to show you a good time, and all we ask in return is that you tell your family and friends about us when you get home. You can do that, right?

If so, we're just going to ask you a couple of questions to see if you qualify, and then we'll have you speak to a free cruise vacation specialist. They'll take down your credit card information, because you will need to pay for the port taxes of around $65.

What do you say? Sound good? Or suspicious? Would you give your credit card info to this "free cruise vacation specialist" from "Grand Caribbean Cruises"? (Those first two paragraphs, by the way, are a rough transcript from a recent phone call we read about.)

Surely you would never believe it when a strange number calls you up and offers you a free cruise. But those calls keep getting made, so they must be worthwhile for someone to put all the time and effort into them, which means that *somebody's* falling for it. We hope it's not you, but it's not just free cruise calls you have to avoid. There are IRS calls, credit card calls, warranty calls, bank emails, Facebook hacks, and too many others to list.

We've written about scams before, but it's such an important topic that, as long as the scammers keep trying to hurt you, we're going to keep trying to protect you. To that end, this article aims to do three things:

1) Show you some examples of the more popular scams being used today
2) Best practices to avoid falling prey to them
3) What to do if you have fallen into a scammer's trap

How To Recognize a Scam

One other call we have personally received numerous times is from a friendly young woman who sounds very concerned about the fact that our automobile warranty will soon be expiring. In her call, she offers to congratulate us on our $1,000 instant rebate and free maintenance and oil change package that we have earned for being a loyal customer. A loyal customer to whom? Alas, she never says, but all we have to do is call her back and hand over some personal and/or financial details, and she'll take care of the rest.

These are a little more malicious than the free cruise offers because the scammer that calls you might actually know that you drive a 2014 Toyota Camry, if your state happens to have publicly-accessible property information like that.

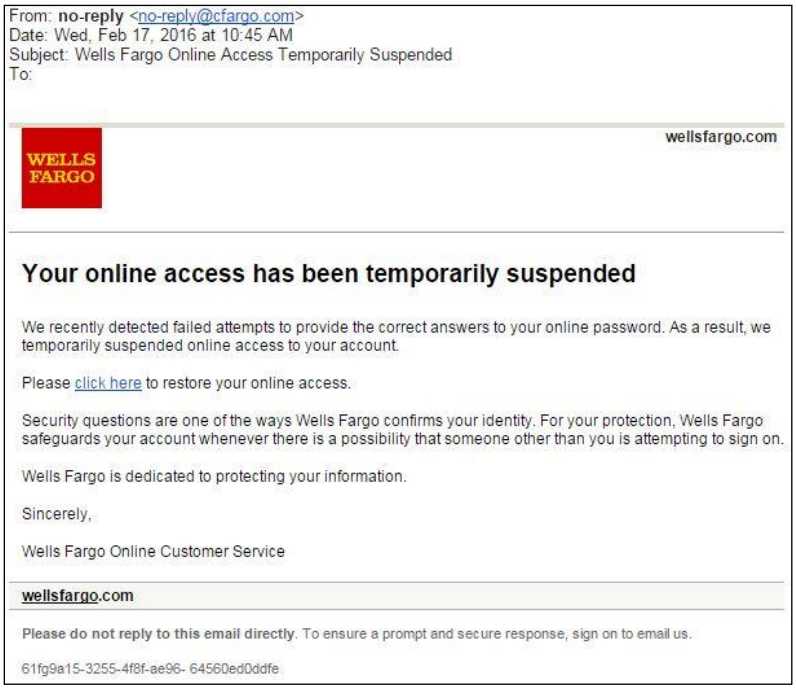
Other scam calls you might receive could purport to be from the IRS ("you must pay us $350 via debit card in the next 4 hours, or the local police will come to your door to arrest you!") or "the credit card reward center from Visa Mastercard."

In this age of smart phones, scammers have begun reaching out not just by voice calls but by text messages as well. Two particularly insidious ones we've seen recently go something like this: you get a text from some long weird corporate-looking number that urges you to respond.

> Today 9:55AM
> **AT&T**: Your account has been charged USD500 for data use. Is this a wrong charge? Text 500 send to 2936XXXXXXX for REFUND

> Today 3:00PM
> **User #25388**: Your Gmail profile has been compromised. We have deactivated it for your protection. Text back SENDNOW in order to reactivate your account.

Or perhaps you might receive an email from your bank advising you that online access to your accounts has been temporarily suspended, and asking that you click a link in that email to have it restored. Here's one claiming to be from Wells Fargo:



From: **no-reply** <no-reply@cfargo.com>
Date: Wed, Feb 17, 2016 at 10:45 AM
Subject: Wells Fargo Online Access Temporarily Suspended
To:

wellsfargo.com

WELLS FARGO

Your online access has been temporarily suspended

We recently detected failed attempts to provide the correct answers to your online password. As a result, we temporarily suspended online access to your account.

Please click here to restore your online access.

Security questions are one of the ways Wells Fargo confirms your identity. For your protection, Wells Fargo safeguards your account whenever there is a possibility that someone other than you is attempting to sign on.

Wells Fargo is dedicated to protecting your information.

Sincerely,

Wells Fargo Online Customer Service

wellsfargo.com

Please do not reply to this email directly. To ensure a prompt and secure response, sign on to email us.

61fg9a15-3255-4f8f-ae96- 64560ed0ddfe

Though we could go on like this for many more pages, we'll leave you with just one more. If you ever receive a weird message through Facebook from one of your friends, it might be a scam. The scammer may have gained access to your friend's account and then begun sending messages to each of that victim's friends. Perhaps they'll claim to be stuck in London and in need of an immediate wire transfer of funds because of some emergency, or perhaps they'll need bail

money ASAP, or maybe they'll even try to help you claim some government grant money that is just waiting for you to ask for it.

Best Practices Part I: How To Avoid Scams in the First Place

So that's a small smattering of all the many scams that are out there waiting to separate you from your money. But what can we do to protect ourselves from being victimized? What are the best practices for avoiding scams in the first place? We have some tips.

First, **never click on a link in an email** unless you are absolutely sure it's from a trusted source. As an example, if you were to receive an email like the one shown above from Wells Fargo, do not click on the link in the email! Call your bank, or use a web browser to see if you actually can access your account. But whatever you do, do not click on the link, *no matter how official the email looks*. A few years ago, scammers had poor grammar and syntax and used out-of-date, if any, corporate logos, but they're getting better and better as times go by. Some of today's slickest scam emails are nearly indistinguishable from actual honest-to-goodness communications from your bank.

And speaking of calling your bank, **never call the number given to you in an email!** You may save yourself from spyware or malware on your computer by not clicking a scam email's link, but if you call the scam email's phone number, then you've still fallen into their trap. If you're going to call your bank, call a number that you either already know or can verify by looking on their actual website.

And speaking of phone calls, if you do ever pick up a call from an unknown number, and if the person or robot who begins speaking sounds the least bit suspicious, **just hang up.** Do not press 1 to be "taken off their call registry," do not say anything, do not keep listening to their scammy spiel. Just hang up the phone and go about your day. If it's on a cell phone, you can block the number if you want, but most of these scammers use dozens if not hundreds of fake numbers anyway, so they'll probably figure out a way to call you again one day.

Hang up even if the call sounds scary. Some scammers pretend to be the IRS hounding you for money. According to its own website, the IRS will never "call to demand immediate payment (generally, the IRS will first mail a bill to any taxpayer who owes taxes), threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying, demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed, ask for credit or debit card numbers over the phone, or call about an unexpected refund."

Our final tip is one that you may think not even worth mentioning because of its obviousness, but we continue to hear tales so we will mention it: **never open a file attached to an email unless you're absolutely sure it's safe to do so.** You may be closing on a real estate deal, when suddenly you get an email from an unknown person claiming to be tangentially related to the process with a document attached that needs your immediate attention. You're busy with something at work, so you don't have time to process the fact that your real estate agent never

mentioned a document like this, you just want this whole thing to be done with, so you open what looks like a simple PDF attached to the email. Bad move. It could be spyware, it could be malware, it could be a Trojan horse that kidnaps your hard drive and holds it for ransom payable in Bitcoin or some other cryptocurrency (side note: stay away from cryptocurrencies too, many of those are also scams). Better to save yourself the trouble and verify with someone you know that you should indeed be opening that file.

Best Practices Part II: Pro-Active Steps to Take

So far, all of our tips have been reactive ones (i.e., what to do if you sense a fraud coming on). There are two more pro-active things you can do to stop scammers in their tracks: (1) freeze your credit, and (2) install a good antivirus program on your computer(s).

To freeze your credit, you'll need to contact each of the three big credit rating agencies: Equifax, Transunion, and Experian. Verify your identity with them, and then ask them to freeze your credit. That way, nobody (not even you) can do any of the following in your name: take out a loan, open a new credit card, open a new bank account, etc. If you find yourself in a position where you want to apply for a new credit card, you'll then have to contact each of the three agencies in order to temporarily lift your credit freeze, but we view that hassle as a relatively small price to pay to keep our credit safe. We have done this for ourselves, our spouses, and our minor children.

As for antivirus, there are many good solutions out there. One knowledgeable IT pro we know recently recommended one that his company uses to protect all of its machines. It's called Cylance, and it currently costs $20 per year to protect up to 10 personal computers (Windows or Mac). Neither we nor this IT pro receives any sort of commission for recommending this product, and we are not tech-savvy enough to know which one is the best. So if you don't want to use this one, that's fine. Do your own homework and pick another one, but for goodness' sake don't leave your devices unprotected.

What To Do If You Become a Victim

Even with the strongest protections and the most vigilance, it's still possible that the best of us can get scammed. If it does happen to you, the first step is to admit it and try to get rid of whatever shame you feel as fast as possible. Once you have accepted the fact, here are your next steps:

* **Change all your passwords immediately**. All of them. Every bank, every email program, every brokerage account, every credit card, everything important, even Facebook. With your new passwords, length is the key. It doesn't matter how weird your password is (e.g., using funny symbols like # or @, or alternating between letters and numbers), but the longer it is the better.

* If your sensitive financial information has been compromised, you may need to **contact the fraud department at each of your financial institutions**.

* If your credit card number has been compromised, **get a new credit card number**. Call your card issuer, explain the situation, ask for reimbursement of any fraudulent charges, and then get them to send you a new card with a new number.

* If you haven't already done it, **get two-factor authentication for all of your important logins**. This would be your bank accounts, investment accounts, emails, and other can't-live-without logins. Single-factor authentication is simply a password. By adding in a second factor to authenticate that it's really you (e.g., having the bank text you a one-time code, using a token that regenerates a code every 30 seconds, or otherwise taking a second step using a second device to log in), you'll greatly decrease the odds of a scammer getting into your personal space online.

* Depending on how severe your loss has been, you may need to **call in the law**. If you lost $49 buying some sham warranty on your credit card, you probably don't need to file a police report for that. Just get the credit card company involved, fix the problem, and move on. But if it is something more material, depending on exactly how severe it is you may need to contact either the local police, the Federal Communications Commission, the Federal Trade Commission, or even the FBI.

Conclusion

As long as this planet is populated by humans, there will be scam artists out there trying to do you harm. The Internet can be a dangerous place. Without getting paranoid about it, try to be vigilant in protecting the money you've worked so hard to earn. With the right systems in place, you may never become the victim of fraud. It can happen to any of us, though, so if it does happen, act quickly to minimize the damage that can be done.

Felipe Garcia, CFA
Chief Investment Officer
INKWELL CAPITAL LLC

Aaron Byrd, CFA
President
INKWELL CAPITAL LLC