

[Click to view this newsletter in a browser](#)



Hello!

Great news! We're **not** doing a holiday gift guide. You can find them everywhere (and if you can't, [here's one](#)).

Instead, we're highlighting blog posts from some of our own tech guys, Frank Kao, Matt Kibildis, and Tim Fitzgerald.

Who knew they were such good writers?

- Frank writes about how to stop from being a Grinch
- Matt writes about keeping your digital life safe
- Tim writes about unsecure wireless networks

Scroll down to read these posts. If you haven't already, you can subscribe to our blog [here](#).

Have a great holiday and here's to a happy and healthy New Year.

All the best,

Rafi Kronzon and Josh Feder
Co-Founders

Follow us on Twitter

We're on Twitter every day, with tech tips, trending news, and occasional opinions. Follow [@cartwheelit](#) to stay tuned!



Facebook Fans

We've got a Facebook page with a growing fanbase! [Click below to become a friend](#).



Read our Small Business Blog

We have a blog for small businesses that offers daily tips and discussions. [Click below to read it](#).



How to not be a Grinch this Holiday Season

As we've been told by numerous holiday specials over the years, the holiday season is all about giving. What if you could make a big change in someone's life for the cost of a single present? I want to draw attention to two great ways you can make a difference on a personal level to those that really need it.

To be honest, I've never given much thought to donating to a charity. I've given to a few things here and there, but I've mostly been pushed into contributing to walkathons or school raffles by other folks with more vested interests than I. As far as I'm concerned, I could have just spent all the money on a slot machine; I have no idea where the money actually goes or if it's actually doing good. That's why I'm genuinely interested in two programs that tout transparency as a major selling point. [Modest Needs](#) and [Kiva](#) both encourage giving, but

in different ways.

Modest Needs rigorously vets applications from ordinary people around the US that have fallen on hard times. Many times, it can be something as simple as a single medical payment, utility bill, or car repair that keeps someone from the downward spiral of poverty. Victims of accidents, medical emergencies, and other life-altering crises can post their personal stories, explaining how much money they need and why. Modest Needs rigorously investigates the legitimacy of their claims, and starts directly paying the claimants bills once a percentage of an applicant's goal number is met. Throughout the process, Modest needs will email you testimonials from that applicants so you can follow their progress. It's an intimate, tax-deductible way to help, and you can see exactly what impact your dollars are having.

In contrast, for those of you who are more globally- or fiscally-minded, Kiva lets you invest directly in an entrepreneur in a third world country. Kiva stresses that any money given is a loan, and they expect that those you invest in will be successful and will be able to pay you back. You can see exactly who your money is going to, and when your loan is paid back, you can choose to directly reinvest in a new entrepreneur if you wish. These budding business people can be anything from a seamstress in Paraguay to a farmer in Cambodia. For those of you that run your own successful small businesses, it's a great way to give the same opportunity to others.

You can find out more at [Modest Needs](#) and [Kiva](#).

Read this article in our [blog](#)

Keeping Your Digital Life Safe (Part 1)

There is no doubt that our world of information and business is heading rapidly in the direction of total digitization or storage on electronic media. Green concerns, physical storage limitations, and overall demands of efficiency have caused nearly all pertinent information to be stored on personal computers, servers, and in data centers; gone are the days of cabinets and boxes filled with filing folders and paper records, though you may be able to find relics of such antiquated objects if you search the darkest recesses of your office.

There are two realms in the world of electronic data security. Online data (Internet, cloud) data and local data (i.e. Data stored on your personal computer). In this two-part series, I will begin by addressing data that is transmitted over the Internet.

I am often flanked with questions from clients and family members regarding privacy of information on the Internet.

- "Can someone see what I'm doing?"
- "How do I know if my payment was really processed?"
- "How do I know if my information is safe?"

The truth of the matter is that there always exists the possibility that information can be lost or stolen. However, there is a solution, and it is one of probability.

You can decrease the chances of data loss or compromise to a level where its occurrence is very unlikely. In terms of preventing data compromise on the internet, there are a few golden rules:

1.) Never follow a link in an email to make changes to a credit card. Whether you receive an email from American Express or from Amazon.com, do not click on it. You can always go directly to the website address where you normally pay your bills or purchase products and then handle the matters directly. Following a link or entering information directly into an email is dangerous, as scam artists have become increasingly skilled at

replicating the templates and logos of large companies, so it is possible for you to be redirected to a website that will record your information and send it on its path to identify theft.

2.) Never send explicit login or password information via email. It is undoubtedly quick and convenient to send passwords over email, whether your assistant needs to access a financial statement or your Aunt Ethel needs to upload family photos. However, this practice may pose a great risk to security. You may be wondering why I might imply that Aunt Ethel is untrustworthy, but I can assure you that this is not the case. The unsecure nature lies in the email technology itself. The solution here is to visit a seemingly archaic time period and call the other person and exchange the password on the telephone. It is true that this does not prevent the other person from writing the password on a piece of paper and leaving it somewhere, but it is ultimately more secure than storing the password in an email account that may be visible for anyone to read.

3.) Always obtain a Confirmation Number when completing secure online transactions. When completing tasks like paying monthly credit card or cable bills, it is now somewhat common to receive an email with a confirmation number. However, some services do not offer this feature and in these cases it is always critical to record the confirmation number that appears on the website following the transaction. This will give you the advantage in the unfortunate situation that your payment is disputed, as it allows the payee to immediately track the transaction in question.

4.) Never use your name, address, or birthday for an account or email password. It is very easy to fall into the trap of using identifying personal information for an email password in this age of information that requires one to remember so many credentials. The most secure solution involves making a password that is an obscure reference to your personal life and to put a mix of capital and lowercase letters as well as numbers and symbols in it. For example, a password like Art1ch0k3! works if you really love to dine on artichokes. You should also read our recent [post](#) on passwords.

In the second part of this series, I will address protection of the data files that are stored on your personal computer in both business and personal environments, so stay tuned!

Read this article in our [blog](#).

Three Reasons all NYC Wireless Networks should be Secured

Before I moved to New York City, whenever I reconfigured my home wireless network I'd make it a point of personal principle to keep it "open", or password-free. In a rural or suburban setting, having an open wifi network can seem a neighborly gesture with few potential consequences. People are unlikely to stumble across your network while walking down the street, and if they do, it's unlikely to be more than one or two at a time. Leaving your network unlocked can also be a personal display of trust and safety feelings, like leaving your door unlocked.

In New York, though, feelings of safety tend to correlate strongly to the sturdiness of your deadbolt. You would never leave your door unlocked, and neither should you leave your wireless network unprotected. We at Cartwheel always lock any wireless networks we set up, and here are three reasons why we think you probably should, too.

1. Remember dial-up? Yeah, so do we.

In less-dense areas, it's easy to accept the possibility that someone might borrow your Internet connection at some point, with or without your knowledge. The impact to your own Internet experience is nearly certain to be negligible, and there are probably big parts of your day where your bandwidth is going totally unused. It's no

skin off your back if someone uses a little bit of it.

But in New York, there might be 30 people within range of your router, few of whom you are likely to know. These people also, in all likelihood, have no idea who owns the unlocked network they're using, and they're probably not going to canvass the apartment building looking for you so they can help pay your cable bill or ask if you're trying to watch Netflix.

In fact, at any given time you will probably end up with more than a few people using your Internet connection, divvying up your overall connection speeds amongst themselves with impunity. If you don't mind waiting 5 minutes for Google to load, this might not alarm you. However, if you enjoy doing anything at all online, you're going to have a very difficult time doing those things if there are 5-10 leeches downloading music, reading the Times, and pirating The Dark Knight on Blu-ray while you're sitting in front of your computer shaking your fist. It'll be slow for the freeloaders, too, so you're not really providing much benefit with all of your self-sacrificing generosity anyway.

2. Sharing does not always have anything to do with caring.

One of our favorite things about having a network connecting our various and sundry computers and devices is that we can share files and folders between computers. At home, I can access my media archive from my living room and watch Firefly on my TV while sprawled across the couch or with a group of comfortably-seated friends, even though the files are stored on the computer that lives at my desk. (Anyone who's watched a lot of television while sitting in a desk chair knows that it eventually becomes a competition between the chair and your back: which will give out first?)

If your wireless network is open, though, unless you have pretty rigorous security on all of your shared folders, you're at risk of having those shared files accessed. If you use Windows, you're also at risk for having payloads of viruses and/or malware dropped into those shared folders. You could heavily protect even the least private shared folders on your network, forcing you to enter logins and passwords as a matter of rote -- but why do that when you can have just one password, securing your network with encryption that even the CIA would have a very hard time breaking?

3. Identity theft is serious business

In a world where credit card numbers are electronically passed around like candy -- when you order something over the phone, when you buy things online, or when you're swiping your American Express Black card at the candy store -- it behooves all of us to be very cautious about where our crucial billing details go, and who gets to see them.

Most of us operate under the assumption that when a business we trust asks for our billing information, they're ultimately responsible for using and then deleting that information responsibly. Unfortunately, there's a lot more to it than that. When you swipe your card at a store or an ATM, the swiper is turning your credit card into an electronic record of your credit card number, expiration date, and secret code. Then, it's calling up a computer perhaps thousands of miles of copper wiring from you, and then actually "speaking" that information aloud in robotese. A bad robot -- er, computer -- could conceivably be programmed to overhear this conversation and steal your credit card data whilst whistling and pretending to read the newspaper.

Fortunately, we don't need to worry about that happening, because when we use a credit card swiper, our data goes through a process called encryption, which makes sure no one in between our ATM and our bank can understand those numbers. A password-protected wireless network relies on precisely the same technique -- and an open wireless network is susceptible to the very same type of snooping. Submitting credit card numbers through an encrypted connection is much, much safer than speaking them over the phone.

[Lifehacker](#), which is a blog I'd recommend to anyone regardless of technical prowess, recently [highlighted](#)

[one more trick](#) that hackers can use to steal data via an open wireless network. It's actually really simple, using a Firefox plugin to steal logins and passwords for unencrypted sites. You can get yet [another Firefox plugin](#) to tell you that someone is using such dirty tricks on the network you're using... or, you can just password protect your wireless network already. For crying out loud -- haven't we given you enough reasons yet?

Read this article in our [blog](#)

We respect your time and privacy. If you no longer wish to receive news, alerts, or promos from Cartwheel, please reply to this message with "Unsubscribe" in the subject line or simply click [Unsubscribe](#)

Cartwheel
6 West 18th Street, 2nd Floor
New York, New York 10011

[Read](#) the VerticalResponse marketing policy.

