

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



Hello!

Summer is in full swing. We hope you're loving it as much as we are.

While this is relatively quiet time for us at Cartwheel, we're busy doing some exciting things like improving our service offerings to you and updating our website. Stay tuned for more details.

Also, if you're on LinkedIn, please make sure to [follow us](#) for upcoming exclusive content!

In this newsletter we bring you the following from our blog:

- The Three Security Breaches you should worry about (scroll down)
- Antivirus for the Mac? The Verdict (scroll down)

Here's a few more that you should check out:

- Microsoft Office 365: Is it for you? ([read](#))
- Google Chromebooks for small business([read](#))
- Could Square be the Answer? ([read](#))

If you haven't already, you should [subscribe](#) to our blog.

Have a great month!

All the best,

Rafi Kronzon and Josh Feder
Co-Founders

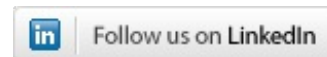
Follow us on Twitter

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



LinkedIn Users

We've got a LinkedIn page. Please follow us for unique videos, reviews and pics!



Read our Small Business Blog

We have a blog for small businesses that offers daily tips and discussions. Click below to read it.



The Three Most Common Security Breaches for Small Business

Perhaps you've been following the recent media frenzy regarding so-called hacktivism (hacking with a social purpose) by groups such as Anonymous and LulzSec.

If you have, you know that they have shown that many of the world's computer servers and secure networks are open to some kind of attack or exploitation if someone tries hard enough. While this has been widely

acknowledged for quite some time – anyone remember [Vladimir Levin](#)? – recent attacks have awoken public paranoia.

When it comes to security, we're pragmatists. While everyone's personal and business information is critical, much of it is immaterial to everyone else. Our approach is to identify the most likely potential incidents and make sure to plug those holes.

For small businesses, these are the three most common security breaches:

1. An employee leaves your company on poor terms and either deletes important files or takes proprietary information with him or her.
2. Someone in the company opens a malicious email or installs a bogus program, thus exposing the network and alerting hackers to a compromised network.
3. Someone in the company loses a laptop or smartphone that contains the company's information or passwords.

With these three threats in mind here is a short list of our recommendations for most small businesses:

1. Have a clear set of procedures for departing employees: This includes disabling accounts, forwarding emails, etc.
2. Educate all employees on how to avoiding malicious email and software. Only install necessary software from trusted sources that you initiate.
3. Firewall: Keep a deep-packet-inspection firewall – one that scans all incoming traffic for threats.
4. A good password policy: Use strong passwords, and use different ones for each employee and application
5. Keep computers up to date: Apply all operating system (Mac, PC, and smart phones) and application patches regularly.
6. Keep entry passwords on all mobile devices.
7. Encrypt hard drives on mobile laptops.
8. Protect your wireless networks.

Keeping with these basic rules will go a long way to keeping you and your company's proprietary information safe.

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

Antivirus for the Mac: The Verdict

Back in 2008, Apple made a [recommendation](#) that Mac users should get antivirus software. Strangely (but not surprisingly), the recommendation is no longer on Apple's web site, and they haven't addressed the matter since. The most common arguments for or against antivirus are:

- You don't need it, because Macs have much better security and people can't build malware (viruses or spyware) for them.
- You do need it, because Macs aren't more secure at all.
- People don't write malware for Macs because there aren't enough Macs for them to bother.
- You don't need it, because an Administrator password is needed to install software on a Mac.
- You do need it, because malware can steal your personal information on Macs without installing.

What to do? We like to think of installing antivirus on a Mac as the equivalent to taking antibiotics without an infection. Sure, it may stop an infection at some point in the future, but the risks of side effects (slow, bloated software that drives you nuts) outweigh the benefits. This is in stark contrast to a PC, which is by comparison a

veritable Petri dish of blood curling deadly bacteria.

We therefore **do not** recommend installing antivirus on Macs at this point. The only exception is if the Mac user is somebody who really has no clue or self-control when it comes to opening Viagra emails and installing every program they see; for example an adolescent child.

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
US

[Read](#) the VerticalResponse marketing policy.

