



# Quantum Computers

We Make It Personal

## April 2011 Tech Tip Newsletter!

April 2011

Issue: S0018



Greetings everyone! I hope you are enjoying this lovely spring season!

It has been a very busy Spring for us at Quantum Computers. In fact, at the time of this writing, most of our team is in Los Cabos, Mexico attending The Congress of Quantum Masters. I am anxiously awaiting their return on April 18th.

For the main article this month I want to share with you an article I read at Norman.com. We continue to see many people impacted by Malicious Malware. I know you are going to find this article helpful in educating yourself and keeping your system safe from attacks. Being educated is the best way to protect yourself! Don't let being "computer illiterate" be your excuse anymore. Get educated.

"Ask Jon" is also a great way to get educated in small easy to swallow bites. This month Jon is addressing a question regarding firewalls.

If you haven't done so yet, make sure you take a look at our Spring Super Sale.

Happy Spring Wishes,

Stefanie Swartzendruber  
Quantum Computers LLC  
[stefanie@qclaptops.com](mailto:stefanie@qclaptops.com)

"Treat your password like your toothbrush.  
Don't let anybody else use it, and get a new  
one every six months."

**[PLEASE CLICK HERE  
TO VIEW THE TECH  
TIP NEWSLETTER AS  
A BLACK AND WHITE  
PDF](#)**

### ***In This Issue***

[Shamelessly Exploiting  
Disasters](#)

[Ask Jon](#)

[Submit Your Own Question](#)

### ***Quick Links***

#### ***Computers & Accessories:***

[Quantum Computers LLC](#)

#### ***Biofeedback Industry Links:***

[The Quantum Center of  
Excellence](#)

[iNDIGO & SCIO Practitioner  
Database](#)

[The Quantum Academies](#)

[Eternale Alliance](#)

[INDIGO System](#)

[SCIO USA](#)

[BHO](#)

#### ***Other Complementary Health Products:***

[The BioMat Company](#)

[Awareness Life Products](#)

[The Quantum Wave Laser](#)

[Kangen Water](#)

[The Alkalizer](#)

- Clifford Stoll

# Shamelessly Exploiting Disasters

An article written by and posted at [www.norman.com](http://www.norman.com)

## Introduction

In previous security articles, we discussed the fact that cybercriminals use big events to spread malware. There are two types of events that are used - recurring (e.g. Christmas holiday, Valentine's Day) and new (celebrity issues, disasters).

Not surprisingly - nevertheless disgusting - the recent events in Japan have inspired shameless exploitations by cybercriminals.

In this security article, we shall examine some of the techniques that are used.

## General Characteristics

Seen from a cybercriminal's point of view there are some characteristics about events that should be noted:

- Incidents that are unforeseen are ideal for malicious activity than recurring events. The former have some special advantages, as we shall see below.
- The more focus an event gets, the better suited it is as a vector for malware.
- News variants offer additional attack options.

The catastrophe in Japan has at least three different aspects that a cybercriminal may focus upon:

- The first huge earthquake (and subsequent earthquakes)
- The tsunami caused by the earthquake
- The nuclear disaster

Jusuru

NRG Bio-Imprinter

Quantum Computers LLC

4448 A Williamson Rd

PO Box 123

Bridgeport, Michigan

48722

Phone: 989-777-5700

Fax : 989-777-4700

Standard Hourly Labor

Rate: \$60

Email:

[support@qclaptops.com](mailto:support@qclaptops.com)

[www.quantumlaptops.com](http://www.quantumlaptops.com)



## Ask Jon...

Dear Jon,

My virus protection software came with a firewall and now I get all kinds of annoying pop ups asking me for permission. I don't know what to allow and what to deny. Help!

Dear Reader,

Those annoying pop ups are performing a very important function. Let me help demystify this a little so you can start looking at those pop ups as your friend.

Rather than go into all the details of what a firewall is and how it works let me just give you a couple rules to help you navigate those pop ups.

First, when a firewall notification pops up, think about what you were doing



These three - and variants - can be used by the cybercriminal in order to trick innocent users. The ultimate goal for the cybercriminal is almost always monetary. Her way to accomplish this goal is to trick users to perform actions that have consequences that are different than the users expect.

The general system may be divided into a series of events like this:

1. Trigger the user's interests.  
*The trigger may be an email, a Facebook posting etc.*
2. Trick the user into performing a particular action.  
*Such an action may be to click on a link, and opening an email attachment, to mention just two examples.*
3. Exploit the potential that has manifested itself from the user's action.  
*Examples are selling personal information obtained, and using the user's computer as a zombie in a botnet.*

## Techniques used to exploit the disasters in Japan

Below are some examples of techniques used by the cybercriminals to exploit the tragedies that have fallen upon Japan. Note that these are only **some** of the tricks used - new variants will appear as long as the events in Japan are top of the news.

### SEO poisoning

One technique particularly useful for cybercriminals, who aim to take advantage of new events, is called Search Engine Optimization (SEO) poisoning. We have discussed this in previous security articles see e.g. [this item](#).

The simple explanation of SEO poisoning is that one manages to get particular web pages high on the results list by using particular techniques.

A search using e.g. Google with words associated with the disaster in Japan, most likely results in an immense number of hits. Several of these are probably fake news pages, which are set up by cybercriminals aiming to infect visitors' computers or attempt to trick you by other means.

just prior to the pop up. Did you ask your computer to execute a function that may require it to connect to the internet? If so, you want to allow that function. So click allow, or yes, or accept, etc. so your computer can continue executing the task you have set for it. If you select "always allow" your firewall will know that this is always okay and will not ask you again.

Second, if a firewall notification pops up for no apparent reason TAKE HEED. Carefully read the popup and when in doubt CLICK DENY. Your virus protection software can't prevent infection of a virus if you have specifically (all be it unwittingly) allowed it onto your computer.

If you'd like more detailed information about firewalls you should consult the user manual for your specific virus protection software. We use and recommend Norman. Here is a link to the manual for the very popular Norman Security Suite.

---

**SUBMIT YOUR  
OWN QUESTION  
HERE!**

---

One typical brand of malware that is propagated by this technique is fake antimalware. SANS' Internet Storm Center has published a very good analysis about the techniques those behind fake antimalware use to poison search engines, and how they are able to be so quick whenever a new incident occurs.

## **Spammed fraudulent emails**

Another variant using the email attack vector is the one that attempts to trick you into donating money.

The fraudsters will often use the name of legitimate, respected organizations - like the Red Cross and UNICEF - and provide links to web sites that resemble the real sites.

Money donated through this type of fraudulent donation sites, will not reach the victims, but the cybercriminal that set up the scheme. The personal information that you were tricked to enter - e.g. credit card information - may subsequently also be abused by cybercriminals.

One such fraudulent email appeared to come from the British Red Cross, which subsequently set up a warning about fake donation requests. One paragraph from the British Red Cross' web page with useful information reads:

*Unfortunately there are currently some fraudulent emails circulating claiming to be raising money for the Japan Tsunami Appeal, please be aware we will never ask for people to donate through companies such as Western Union or Money Bookers.*

## **Attacks using social networks**

Social networks have in recent years, been one of the most successful and thus popular attack vectors.

There are numerous examples of clickjacking - or likejacking - postings on Facebook. One of these claims to show a video of a whale that are launched into a building by the tsunami.

## **Spammed malicious emails**

Email is still a useful and popular technology for cybercriminals. If they succeed in tricking a sufficient number of recipients to click on malicious links and/or open malicious attachments, this is a low-cost and well-proved technique. Spammed emails are often used in combination with the other attack vectors mentioned above.

## **SMS hoax**

Among the more peculiar fake messages is an SMS message that spread in the Philippines and other countries close to Japan in soon after the nuclear radiation problems were reported. The message was *Radiation may hit phil starting at 4pm today. Pls send to ur loved ones*

It soon became clear that the message was a hoax. Nevertheless, it was reported that schools sent their students home in order to avoid

radiation.

The motivation behind this type of message remains obscure unless its origin was due to a misunderstanding and not intentionally meant to cause distress.

## Avoid being a victim

Clever, targeted attacks are almost impossible to protect against. However, the attacks that utilize disastrous events are rarely targeted, and you should be able to implement security mechanisms in order to avoid being victimized.

You should of course have updated malware protection software and firewall in place. Other security software may ensure increased protection. Exploitation of software vulnerabilities is a very common technique to get malware installed on your computer, and it is therefore imperative that you update your operating system and software as soon as possible after the vendors have published security patches.

In our two-part article

- [Self-protection from malware - part I](#)
- [Self-protection from malware - part II](#)

you will find useful suggestions on how **you** can protect yourself against malware. The single most important measure is to **increase your own awareness**

**PLEASE NOTE:** At Quantum Computers, our primary customer base is with Complementary Alternative Health Practitioners, mostly in the field of Biofeedback. Some of our articles may seem confusing to people who are not Biofeedback Practitioners, however we do try to write articles that are beneficial for everyone.

## Join Our Mailing List!

Spring Super Sale

Spring, 2011

.....

### Super Laptop Deals

Whether you are looking to replace your main computer for biofeedback, want to protect your business with a backup computer, or want a great portable laptop for yourself or a student, WE HAVE THE PERFECT LAPTOP FOR YOU! Check out our great computer deals for Spring by clicking on the picture to the right!

There are two models that Ron is especially excited about! One is the QCW150 designed for the budget conscious practitioner. The second is the QC170HM Dream Machine. We just can't get Ron to stop talking about these computers! And if he is excited you should be too. Take a look and see for yourself.

---

### Super Biofeedback Accessories

Accessories are a great way to build your business. You'll see enhanced results and be able to address client specific issues by taking advantage of the many specialized accessories created just for the biofeedback industry. Now is the perfect time to add a new accessory to your practice.

---

### Super Spring PC Cleaning Services

Spring means Spring Cleaning and at Quantum Computers that means cleaning up computer software. Whether you just need some routine maintenance or are experiencing a problem that needs some serious attention we have the right service for you. Take advantage of our Super Sale to get computer running smoothly for Spring!

---

### Spectacular Dermagetix Sale!!!

If you've never tried Dermagetix NOW IS THE TIME! If you know it and love it (and we know you do!) NOW IS THE TIME TO STOCK UP!

This sumptuous organic skin care line is profoundly effective by itself and even more fabulous when enhanced with frequencies from the test plate on your biofeedback device.

These amazing discounts will NEVER BE LOWER! So take advantage of these saving now and see just how youthful your skin can look and feel!

---

**Save  
10%**

Can't find what you need in the Spring Super Sales section? We've got you covered! We'd like to offer you 10% Off any REGULAR PRICED item in the BIOFEEDBACK ACCESSORY category on our website. Just use the coupon code below when placing your order. You may click on the link above to be taken directly to the BIOFEEDBACK ACCESSORY page. Coupon code is only applicable to items in this category.

**Offer Expires: April 18, 2011**

**COUPON CODE: SUPERSPRING**

