

## Bryley Tips and Information December 2009

### **1. Social Media and the New Wave of Brand Damaging**

The growth and popularity of social media, as well as its recent transition from strictly personal accounts to valuable business-marketing tools, is hard to ignore. Suddenly, every business is Tweeting and setting up a Facebook account. But, in addition to business communications, social networking opens up a new channel for brand attack: Spreading malware, reputation slander or brand bashing, and imposter sites that divert traffic away from your site are the most common concerns.

Online counterfeiting is another form of brand attack commonly found in social media. An example was provided in COMPUTERWORLD'S October Article *Scams & Shams: The Trouble with Social Networks*: Pirated copies of Microsoft's Windows operating system were being sold online, and some people who bought them, thinking they possessed legitimate copies, received software that often contained embedded spyware and malware. Not only did the users blame Microsoft for problems caused by the malware, but the counterfeiters probably made more money from the spyware and malware than they did from selling the pirated software itself.

So what defensive moves should you employ to protect your brand? As with domain names, one should register their company, brand names, and trademarks on the major social-networking sites. On top of this proactive measure, one should also engage their marketing team in reactive strategies, such as social-media investigations for cybersquatters. For example, Kodak hired a "chief listener" whose job is to monitor all online conversations regarding Kodak, routing all problems – legal, marketing, IT problems – to the appropriate groups so that the company can formulate the appropriate solutions.

Some threats are even self-inflicted. Companies may accidentally hit "send" instead of "save" and put information out too early. Employees post comments on social-media sites regarding practices at the company that they do not agree with.

Your final defensive tactic should be to monitor closely what you and your employees are posting, making certain that it is quality content only. Remember, with so much online activity to monitor, it is important to prioritize. According to Lynn Goodendorf, global head of data privacy at the U.K.-based InterContinental Hotels Group, you should focus on your most sensitive and confidential data and mitigate your largest exposures.

Learn more at COMPUTERWORLD: *Scams & Shams: The Trouble with Social Networks* at [http://www.computerworld.com/s/article/342446/Scams\\_Spams\\_Shams?source=CTWNLE\\_nlt\\_dailyam\\_2009-10-19](http://www.computerworld.com/s/article/342446/Scams_Spams_Shams?source=CTWNLE_nlt_dailyam_2009-10-19)

## **2. Join the Social-Media Crowd, but Beware of Facebook Phishing!**

We recommend that you step forward into the new generation of Inbound Marketing and enter the realm of Social Media. Get Tweeting, link in to LinkedIn, and create that Facebook page. This is the future of your company's marketing ventures.

Just be aware of the new threats contained within these online business networks. A very pervasive threat today for businesses on social media sites is phishing. (Phishing, in the field of computer security, is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit-card information by masquerading as a trustworthy site.)

One of the largest threats of this kind today is a counterfeit Facebook page that launches both a phishing scheme and a banking Trojan on the user's computer. This malware campaign, according to ChannelWeb writer Stephanie Hoffman, is part of the global Zeus botnet (Zbot for short) which is delivering about 1,000 phishing messages per minute per domain over about 30 domains, translating into 30,000 installed messages per minute. These messages appear to be from Facebook, and attempt to trick users into surrendering up sensitive personal identity and financial information.

How can your company avoid this particular phishing scam? Alert your employees of its existence and educate them on its design. The attack will appear as such:

- Facebook users will receive an email informing them that Facebook is updating its login system to further enhance security.
- The scam will then prompt users to click on a supposed update button embedded in the email. If one were to click on this link, they would be directed to a phony Facebook login page where their username is already convincingly filled in for them.
- They are then asked to type in their password to allegedly complete the update.
- After logging in, users are then directed to another page that prompts them to click on the "update tool" which in actuality is the Trojan updatetool.exe; clicking on this tool infects ones computer with the Zeus Trojan, notorious for targeting banking accounts.

Researchers at the security company AppRiver suggest that this is enough for to recognize this scam in particular and any others in general as no credible entity on the web – Facebook, your personal bank, et cetera – needs the participation of every one of its users in order to update their product. Protect your PC, your personal identity, and your financial information; remain constantly vigilant. Know that these scams are out there and avoid clicking on links embedded in emails if you do not know the sender or find the email phishy in any way.

Learn more about Facebook imposter sites, their damaging effects, and how to spot them at CRN ChannelWeb: *Facebook Users Targeted by Banking Trojan*. This article can be viewed at <http://www.crn.com/security/221100165;jsessionid=IBV3UJVFWA5O5QE1GHRSKH4ATMY32JVN>

### **3. Annual Data-Backup Guidelines**

Each December, Bryley publishes its *Data-Backup Guidelines* for the upcoming year. Authored by Mike Carlson, Bryley's Chief Technical Officer, this document details:

- The Importance of Backups
- Backup Technologies
- Daily Procedure – Tape-Based Backup
- Tape-Based Backups and Scheduling

It includes a Backup-Rotation Calendar and a Backup-Event Log, both handy guides for tracking tape backups.

To download your free copy, visit [www.Bryley.com/news\\_and\\_events-newsletter.html](http://www.Bryley.com/news_and_events-newsletter.html).

### **4. Announcements, news, and events**

Follow Bryley Systems on Twitter – Visit <http://Twitter.com/BryleySystems>.

Friend Us On Facebook – Please goto <http://www.facebook.com/pages/Bryley-Systems-Inc/176028273181?ref=ts> to friend Bryley Systems.

Monthly service-ticket survey drawing – We hold a drawing each month for those who respond to our service-ticket surveys. (The survey is announced at the bottom of each email notification on the completion of a service-ticket.) Winners are announced in *Bryley Tips and Information*.

Free webinars on Intelligent Communications – Join us for an enlightening discussion on Intelligent Communications and how it is transforming businesses around the world.

These sessions are sponsored by Avaya Inc., a world-leader in communications solutions. Bryley Systems, an Avaya Business Partner, is fully versed in these solutions.

Please register at <https://secure.avaya-news.com/ats/show.aspx?cr=122&fm=437>.

\*\*\*\*\*  
Client service

If you have questions about, or issues with, our client service or response, please contact Beverley Denio, Client-Service Manager, at 978.562.6077 x201, or Gavin Livingstone, President, at 978.562.6077 x215. (Respective email addresses are [BDenio@Bryley.com](mailto:BDenio@Bryley.com) and [GLivingstone@Bryley.com](mailto:GLivingstone@Bryley.com).)

#### Bryley's Client-Service Portal

Over the past years, Bryley has made significant investments in our business systems and infrastructure to enable real-time communications regarding the timeliness and quality of services we deliver. A result is that client-service requests (with resulting service tickets) may now be added, viewed, or updated through our Client-Service Portal.

This real-time environment is available 24 x 7 at [www.Bryley.com](http://www.Bryley.com) by selecting "Client Login" from the upper-right corner of the home-page. Registered users may perform these functions:

- View the current status and details of their service tickets

- Enter new service requests
- Review invoices
- View reports

To use this capability, please contact Beverley at 978.562.6077 x201 to setup a username and password. Training is also available at no charge.

\*\*\*\*\*

## Contact Bryley Systems Inc.

Bryley Systems is a full-service, end-to-end provider of business-technology solutions, fulfilling the information-technology needs of organizations throughout New England since 1987. Areas of expertise include:

- Managed Technology
- Computer-network performance and reliability
- Network security
- Unified Communications

Email: [Info@Bryley.com](mailto:Info@Bryley.com)

Phone: 978.562.6077

Fax: 978.562.5680

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

Bryley Systems Inc.  
12 Main Street  
Hudson, MA 01749-9990

*Business Technology Solutions Since 1987*

\*\*\*\*\*

## How to Subscribe or Unsubscribe

Bryley Tips and Information is a free e-newsletter sent each month (except July). It provides information and user-level tips on computer and telephone-system issues.

You are receiving this e-newsletter because:

- You are a Bryley client
- You have received a quote or proposal from Bryley sales, or
- You have had business contact with Bryley Systems.

### Subscribe

If you or a colleague wishes to subscribe to this e-newsletter, please e-mail [Newsletter@Bryley.com](mailto:Newsletter@Bryley.com), visit [www.Bryley.com/news\\_and\\_events-newsletter.html](http://www.Bryley.com/news_and_events-newsletter.html), or contact Michelle at 978.562.6077 x216 or via [MDenio@Bryley.com](mailto:MDenio@Bryley.com).

### UnSubscribe

Options to unsubscribe from this e-newsletter:

- Please reply to this newsletter with the word “unsubscribe” in the subject header.
- Visit [www.Bryley.com/news\\_and\\_events-newsletter.html](http://www.Bryley.com/news_and_events-newsletter.html).
- Email [Newsletter@Bryley.com](mailto:Newsletter@Bryley.com).
- Call us at 888.280.5799.

\*\*\*\*\*

Copyright 2009. Bryley Systems Inc. All Rights Reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. The information contained in this document represents the current view of Bryley Systems Inc. on the issues discussed as of the date of publication. Bryley Systems Inc. cannot guarantee the accuracy of any information presented.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT. The user assumes the entire risk as to the accuracy and the use of this document.