# WISE GIVING GUIDE™

BBB WISE GIVING ALLIANCE : SPRING 2015

## This is Personal:

## Privacy and Security in Online Giving

BBB
Start With Trust

**A Publication of the BBB Wise Giving Alliance**

The *Wise Giving Guide* is published three times a year to help donors make more informed giving decisions. This guide includes a compilation of the latest evaluation conclusions completed by the BBB Wise Giving Alliance.

If you would like to see a particular topic discussed in this guide, please email suggestions to **give@council.bbb.org** or write to us at the address below.

**SPRING ISSUE 2015**

BBB Wise Giving Alliance
3033 Wilson Blvd.
Suite 600
Arlington, VA 22201
(703) 276-0100
www.give.org

*Wise Giving Guide* Layout and Production — art270, inc.

Publication No. 11-24-503

Staff members from the affiliated Council of Better Business Bureaus, Inc., provide administrative, personnel, media, accounting, information technology, legal and office services to the BBB Wise Giving Alliance.

# INSIDE

## BBB Wise Giving Alliance Board of Directors

## BBB Wise Giving Alliance Staff

**H. Art Taylor**
*President and CEO*

**Bennett M. Weiner**
*Chief Operating Officer*

**Elvia Castro**
*Research Analyst*

**Jean Lewis**
*Administrative Coordinator*

**Edward Loftin**
*Research Analyst*

**Holly Parker**
*Research Analyst*

**Julie A. Rizzo**
*Director, Development & Charity Seal Licensing Program*

**Shawn Van Gorder**
*Director, Charity Evaluation*

**Ezra Vazquez-D'Amico**
*Research Analyst*

# president's MESSAGE

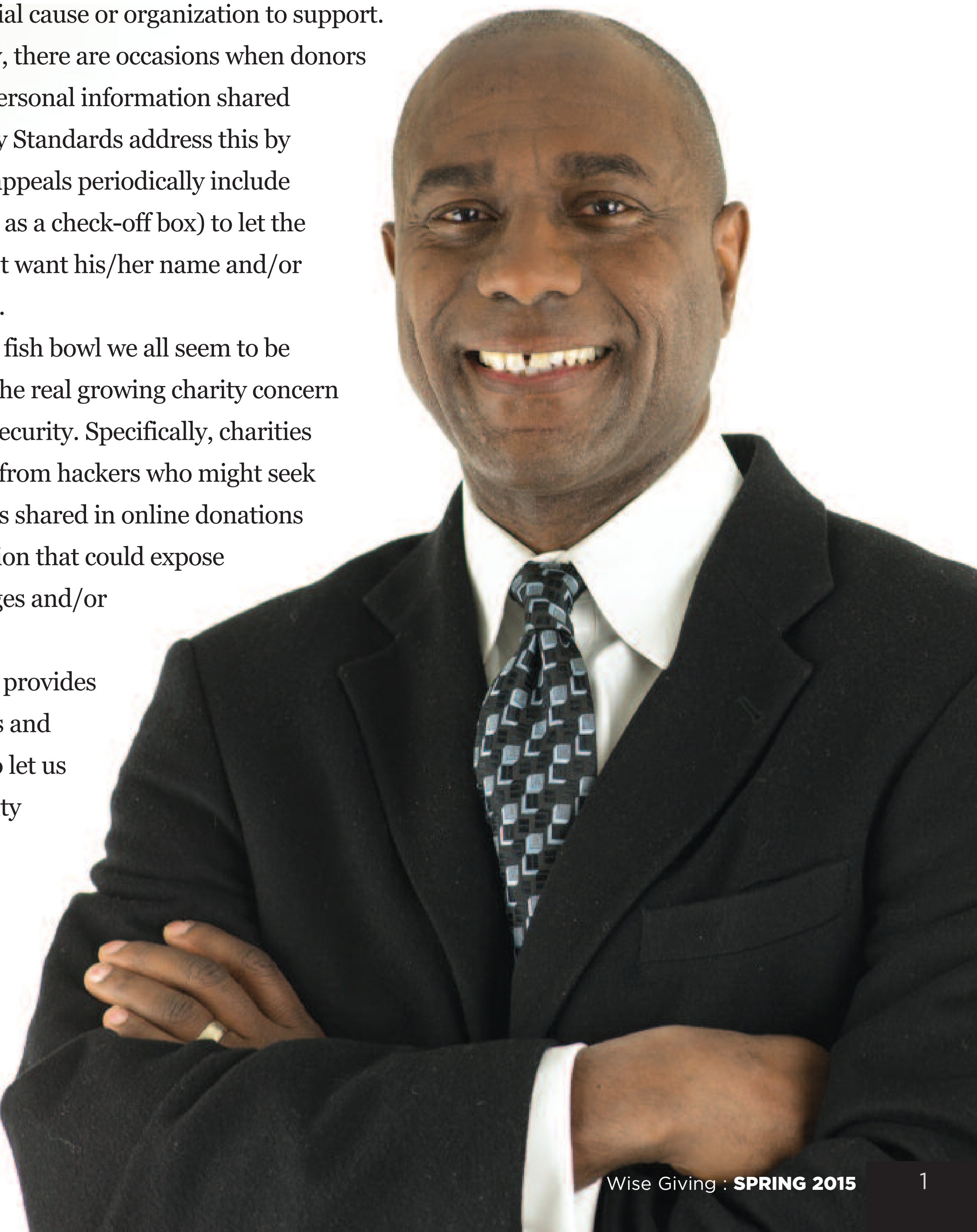
These days a visit to the grocery store or the local pharmacy results in using an individualized card that tracks the selection, date and quantity of every purchase I make. Between this and credit card use, it seems almost every transaction, whether online or offline, is somehow being added to a database somewhere in the cyber universe.

When I make a donation to a charity, however, sometimes I have different expectations. Making a charitable gift is a personal decision, especially if I have chosen a controversial cause or organization to support. So, in terms of donor privacy, there are occasions when donors don't want their name and personal information shared with others. Our BBB Charity Standards address this by recommending that mailed appeals periodically include an opt-out notification (such as a check-off box) to let the charity know that one doesn't want his/her name and/or personal information shared.

Nevertheless, in the data fish bowl we all seem to be floating during this decade, the real growing charity concern is not data privacy but data security. Specifically, charities want to protect their donors from hackers who might seek to access credit card numbers shared in online donations and other personal information that could expose the contributor to false charges and/or identify theft.

We hope this cover story provides useful advice for both donors and charities and welcome you to let us know about what other charity privacy and security issues concern you.

H. Art Taylor, *President*



# This is Personal:

## Privacy and Security in Online Giving

*By Edward Loftin*

**Worm. Bug. Bot.** No, we are not talking about garden pests or the forthcoming Stars Wars film. These menacing monikers are all forms of malware, or malicious software, designed to damage or disable computer functions. Malware can be used to compromise the security of personal information at home and in the workplace. Forms of malware that gather PII, or personally identifiable information, can cause massive financial harm and stress for donors. The consequences of compromised security for the charitable organization can include reputational damage, financial damage, potential legal trouble and perhaps most significantly, loss of donor trust. To avoid these dangers in an increasingly digital age, the privacy and security of personal information must be taken seriously.

In late 2013, criminals gained access to the database of retail giant Target which resulted in a security breach of customer names, addresses and credit card information. Target closed this access to data but not before information was stolen on up to 70 million individuals. In October of 2014, hackers, perhaps with ties to North Korea, caused an international incident when they attacked Sony Pictures, leaking internal documents and emails with fallout ranging from class action lawsuits by Sony employees to major reputational damage. More recently, in January of 2015, large health insurer, Anthem, faced a digital attack affecting an estimated 80 million current or former customers by accessing Social Security numbers, income information, email and street addresses.

While security breaches in the private sector are often well-documented in the media, the charitable sector isn't immune to the malicious behavior of cybercriminals. In February of 2015, respected D.C. think tank, the Urban Institute, was attacked, with criminals accessing email addresses and passwords of up to 700,000 organizations contained in the database of the Institute's Center on Nonprofits and Philanthropy. The breach involved accessing information on users of the Center's IRS Form 990 filing systems. The Center quickly informed the organizations about the incident and urged them to change their passwords. While much of the data obtained in the Urban Institute hack, such as IRS Form 990s, is already publically available, such breaches show that hackers don't discriminate by industry or organization type.

Although direct mail donations still dominate the charitable giving landscape, online contribution transactions are likely to continue increasing. The rise of mobile devices and social media make interacting with charitable organizations easier than ever. Donors and charities alike must take reasonable precautions against digital crime. In this article, we take a look at the privacy and security of personal information as exchanged between donors and charitable organizations. Included will be a discussion of some of the methods used by criminals, the best way for individuals and organizations to avoid victimization, and what to do if a security event does occur.

## Tools of the trade: how cybercriminals attack

Cybercriminals have many tools at their disposal. As noted in Fortune 500 technology company Symantec's (producer of Norton products) *2014 Internet Security Threat Report*, over 552 million identities were breached in 2013, a year termed the "Year of the Mega Breach." These attacks fall into four basic categories:

- Targeted attacks and data breaches;
- E-crime and malware delivery tactics;
- Social media and mobile threats; and
- Phishing, spam and email threats.

***TARGETED ATTACKS*** are aimed at particular organizations or groups typically using "spear phishing" emails by which fraudsters send emails purporting to come from a legitimate or trusted source. "Watering holes" are targeted attacks which make use of malicious code to attack websites frequented by the mark. Of significance to consumers and charities are targeted attacks on point of sale (PoS) systems such as those used in processing retail transactions. According to *Forbes*, an extended targeted attack on a third-party credit card vendor used by Goodwill affected twenty of the charity's members' stores and compromised 868,000 customer credit cards. In addition to other steps, Goodwill launched an investigation with federal authorities, provided a list of affected stores on its website and has since cut ties with the vendor. Data breaches come in many forms, including accidental breaches by the public or theft or loss of computers or drives. However, according to Symantec's 2014 report, hackers were responsible for the largest percentage of reported breaches (34%) and the largest number of identities exposed in 2013.

***E-CRIME*** and cybersecurity terminology may sound like an episode of the *Walking Dead* meets *Battlestar Galactica*, with criminals unlawfully accessing computers to install malware. This turns them into "zombies" that become part of a "botnet" (robot network) that "can be used for a wide variety of purposes, such as sending spam emails, stealing banking information, conducting a distributed denial-of-service (DDos) attacks against a website, or a variety of other malicious behavior." (Norton, 2015) A recent trend in E-crime is ransomware, a type of malware that disables a computer system until a ransom is paid by the victim. In 2014, the Dickson County, Tennessee Sheriff's Office was forced to pay a ransom of $572 to unlock 72,000 files including autopsy reports, witness statements and crime scene photographs using a form of malware called CryptoWall. Norton reports that ransomware activity increased from just over 100,000 infection attempts in January of 2013 to over 650,000 attempts in December of the same year.

> **…over 552 million identities were breached in 2013, a year termed the "Year of the Mega Breach."**

***SOCIAL MEDIA***'s increasing popularity has also caught the attention of cybercriminals. In 2013, 81% of social media threats identified by Norton were fake offers similar to those seen in phishing and spam emails, with offers of "gifts cards, electronics, concert tickets and DVD box sets." (Norton, 2014) Mobile threats have risen with the adoption of the Android platform, which give users "more freedom to install software from outside their official marketplace," but perhaps at the expense of security. Text giving may be safer than giving personal information over the phone since the donor does not have to disclose personal information. The donation is simply added to your wireless phone bill.

***PHISHING*** and spam are among the most recognized cybersecurity threats by the general public. Just about anyone with an email address has received suspicious messages in their inbox. However, remaining vigilant against these types of threats is important as long as criminals are trying to dupe individuals into providing personal information. Also, as the public becomes more knowledgeable about these types of attacks, criminals are likely to increase their level of sophistication (perhaps moving from Nigerian Prince in need of aid to spam email that looks almost identical to a legitimate source). According to the Internet Security Report, 87% of spam emails in 2013 contained hyperlinks. Repeat after me: Do. Not. Click.

No matter the means, cybercriminals are hunting for credit card information, birth dates, government ID numbers, addresses, phone numbers, medical records, financial information, email addresses, and password and login information. Keep in mind that sophisticated criminals can connect the digital dots by using some information such as your name and address to find out additional information.

## Be proactive: cybersecurity for the donor

According to Cindy Leonard of Robert Morris University's Bayer Center for Nonprofit Management, the security of online transactions with charitable organizations is not solely in the hands of the organization itself, saying that it "seems that we place a lot of expectations on companies and nonprofits to keep our data private. But individuals, including donors, need to share in that responsibility ourselves." With this in mind, there are several ways donors can do a better job of taking cybersecurity into their own hands without being technology experts. Spencer Bolles, IT Director at Bay Area Community Resources, mentions some simple steps to protect yourself from cybercrime, asking the question, ***"What does the donor know about the security of their own system?"***

**When interacting with charities through social media, make sure you are dealing with the organization.**

Charities are in a unique situation in that they are held to a higher standard of trust than for-profit businesses focused on their bottom line.

First of all, take advantage of updates. If your operating system offers automatic updates, download them as frequently as they are made available or make sure that feature is turned on. Keep in mind that any frequently-used third party plugins such as Adobe Flash Player or QuickTime need to be updated as well. Additionally, browsers such as Internet Explorer, Firefox or Google Chrome should be updated on a regular basis and can also be set to update automatically (auto update is often the default setting). Also, Bolles points to using anti-malware software to protect your system. Browsers provide the option to clear certain information such as autofill form data and passwords. Bolles points out that while it might be easier to save passwords for the sake of ease of logging in to sites such as your bank or an online store, an unintended consequence is the vulnerability of your personal information. Yes, the password is saved; but it is also stored, and if it is stored it could be accessed by hackers. The effort it takes to find a different method of password storage is likely worth it when compared the damage caused by someone accessing your personal information.

As important as the safeguarding of home computer systems is the way donors interact with charitable organizations and third party donation processors. Bolles points to some common sense questions that can help: "What server are you using to make your transaction? Do you know that you are entering the information for something that isn't fraudulent? Are you sure you're on the website you think you are on?" Web of Trust and VirusTotal are detection services that allow users to enter URLs (web addresses) or links into a tool that analyses the data for the presence of malware. When making on online donation, make sure the third party payment provider (e.g., PayPal, Network for Good) used to process your gift is a name you trust. While bigger isn't always better, it seems reasonable that organizations with experience *and* size would have greater resources to create the safest encryption pathway for your personal information. Never make an online donation unless you feel comfortable.

When interacting with charities through social media, make sure you are dealing with the organization. Don't click on links in communications and make sure to go to the charity's official website to give. Scammers can use social media to piggyback on campaigns such as the Ice Bucket Challenge, and your donation and personal information could end up in the wrong hands. Giving via text message avoids these potential problems since donations are added to your wireless phone bill and don't require you to provide your personal information (though your wireless carrier already has it).

If your personal information is compromised, the Federal Trade Commission (FTC) suggests three steps that should be taken immediately:

- Place a fraud alert with credit reporting companies (Equifax, Experian and TransUnion).
- Order your free credit report from each of the organizations.
- File an Identity Theft Report with the FTC and local police.

These steps will get you started, but the reality is that the process is complicated and will depend on the extent of damage done and may include reviewing your credit reports, disputing errors with credit reporting companies, canceling credit cards and a host of other frustrating administrative tasks. For more detailed information on these identity theft steps visit ftc.gov, justice.gov, or bbb.org/council/news-events/lists/consumers-tips/.

## Mission control: nonprofit cybersecurity

Charities are in a unique situation in that they are held to a higher standard of trust than for-profit businesses focused on their bottom line. With this in mind, charitable organizations should make every effort to protect the security of donor information, whether or not they share this information with others.

What determines what type of charities are best at guarding donor's personal information? According to Cindy Leonard of the Bayer Center, “You would assume that larger nonprofits would be great at privacy and security because of more sufficient funding and staff but that is not necessarily true. Some small groups do a fantastic job and some large groups need to do additional work in these areas.” Leonard points to awareness in upper management and board leadership of the need for robust privacy and security measures: “Does the executive director and board have privacy and security on their radar? If not, those topics need to be addressed.”

After raising awareness, the next logical direction for helping a charity to ensure it is offering the best protection of donor's personal information is to complete an inventory of the charity's current security measures. Such an inventory should include who, what, where, why and when questions about the security plan in place, if any, and the kinds of data the organization collects. Some example of the topics to cover include: payment processors, personally identifiable information, encryption, and sharing of information.

**“You would assume that larger nonprofits would be great at privacy and security because of more sufficient funding and staff but that is not necessarily true.”**

Charities should also develop and implement an online security plan. The FTC's *Protecting Personal Information: A Guide for Business* provides some insight into the items to include, from general network security, password management, laptop security, firewalls, wireless and remote access and security of digital copiers. Organizations must also consider their choice of third-party processing firms in their security plans. Make sure the payment processor you choose takes security seriously. Adherence to the Payment Card Industry Data Security Standards (PCI DSS) is a step in right direction. These standards include 12 requirements focused on network security, protection of data, vulnerability management, access control measures, monitoring and testing maintenance of an information security policy.

In the event of a security breach, having a plan in place will help ensure a rapid response to stakeholders. Spencer Bolles' *An IT Director's Guide to Securing Your Data* provides some useful advice for what to include in such a plan, such as a list of breach team members; an attorney on the team familiar with privacy laws; a forensics team to determine the damage done, and a public and media relations professional. Bolles also mentions that a breach plan would need to include remediation steps "for stopping the breach and preventing it from happening again." As previously mentioned, the security of donor information by a charity is largely a technical matter. But, when a breach occurs, charitable organizations may be subject to disclosure laws that require notification to individuals who have had their personally identifiable information accessed.

The resources for most charities are not on the same scale as private businesses. Nevertheless, donors are trusting charities to do the right thing and protect them from unauthorized access to personal information. Charities could consider cybersecurity as the cost of collecting donations online. Online giving is often touted as being a low-cost alternative to direct mail fundraising since there is no printing, addressing, mail sorting and postage expense. While those expenses are not relevant to online giving, cybersecurity is a definite necessity. In turn, donors must recognize that sometimes significant charity resources may need to be used for cybersecurity protection.

## Between you and me: privacy in online giving

Data security goes hand in hand with privacy, but there are important distinctions between the two. Security deals with the technological, physical or administrative means of keeping information safe. Privacy often deals with the legal and ethical responsibilities an organization has with regard to sharing your personal information. And privacy, unlike security, can sometimes operate differently in the charitable sector than in the private sector. For example the FTC does not have the authority to regulate charities on these issues. Legislation such as the Gramm-Leach-Bliley Act calls for significant privacy measures in the financial services industry, but again does not give the FTC explicit charity oversight responsibilities. In addition, while the Health Insurance Portability and Accountability Act (HIPPAA) provides rules for privacy and security but these are applicable to those receiving health-related goods or services from charities rather than those making donations.

A.J. Zottola, a Partner with Venable LLP's Nonprofit and Intellectual Property Transactions Groups, points out that "what is prudent for a for-profit is prudent for a nonprofit" when thinking about privacy. Zottola also emphasizes, "If you are going to collect personal information through your website, you need a privacy policy, first and foremost." This need is reflected in BBB Wise Giving Alliance Standard 18, which recommends that charitable organizations have a privacy policy on its website containing four elements:

> **The resources for most charities are not on the same scale as private businesses. Nevertheless, donors are trusting charities to do the right thing and protect them from unauthorized access to personal information.**

- What information is being collected and how will it be used?
- How to contact the charity to review your data and request corrections?
- How to indicate one does not want this data shared with others?
- What security measures are in place to protect this data?

Keep in mind that charity data security issues go beyond just credit card donation transactions. Charities might enable people to order personal health materials or invite emails to ask about private matters. This contains information and data that should be protected as well.

## To share or not to share?

The direct mail fundraising model for charities seeking donations in the United States sometimes relies on sharing mailing lists with other organizations. The availability of charity mailing lists is a necessity for newer or smaller charities seeking to develop their own donors for the first time or expanding an existing list of contributors. In turn, other charities count on the funds they can generate from sharing mailing lists as a means of supplementing their revenues.

If you purchase items using mail order catalogs, chances are you are eventually going to be placed on mailing lists of other retailers. The same principle applies to charitable solicitations. Of course, some charities choose never to share their mailing lists under any circumstances and usually state this in appeals if that is their policy. However, for those that do share mailing list information, BBB Charity Standard 18 calls for direct mail appeals to periodically include a notification, such as an opt-out check-off box, that enables donors to easily inform the charity that personal information should not be given to outside parties.

Today's information age presents both opportunities and new challenges for charities and donors. We can quickly access charity websites and check out charities with a click to Give.org. The potential promise of providing a lower-cost method of fund raising than traditional direct mail efforts can be a reality for more charities but only if this can be accomplished with safety and security. Donor trust, once lost, is most difficult to recover. BBB WGA has seen this hurdle occur again and again when previous fund raising methods have engaged in questionable practices. If online fund raising learns this lesson from offline development efforts, perhaps it can avoid some of the pitfalls and strengthen trust while online fundraising further evolves and develops. ■

Donor trust, once lost, is most difficult to recover. BBB WGA has seen this hurdle occur again and again when previous fund raising methods have engaged in questionable practices.