

# Protecting charities from online fraud



Commerce Media's Michael Robertson – the recent series of high profile data losses in the public sector should be a wake up call for senior managers in charities.

**MICHAEL ROBERTSON**, managing director of **Commerce Media**, explains the threat to charities from malicious online activity and how charities need to adopt the new security techniques available.

The Internet has provided charities with a whole new way to communicate with their members and other stakeholders at a local, national and global level. The ability to convey a message to millions of people through a single email or website posting is a supremely neat and cost effective solution in an environment where every penny counts.

Web technology has created virtual communities who can share information and donate money. Charities are tapping into the public's familiarity with the medium by raising funds in innovative ways like online lotteries and bingo, and many are becoming significant e-retailers where both members and non-members alike can purchase a wide range of cause related goods from branded websites.

Aside from fundraising, the Internet has enabled organisations to keep their volunteer networks informed and involved, for example by allowing volunteers to access – and in some cases upload – often sensitive data whilst working away from head office systems. There are also specialist websites for charity managers which help them streamline management processes in areas like e-procurement.

## exposes

**A SOFT TARGET.** Although opening up their networks to facilitate the exchange of information across a wider range of stakeholders offers many opportunities for charities, it also exposes them and users of their websites to an ever-growing number of sophisticated e-crimes, such as financial fraud and identity theft.

Traditionally the brunt of such activity has been borne by the financial sector, especially online banking and high value e-commerce sites. However, as these industries begin to get on top of the problem through public awareness campaigns and tighter controls, e-criminals are moving to softer targets.

Charities have become targets because of the value of online financial transactions they now host and the amount of individuals' private data they have captured for research and marketing purposes.

Phishing, pharming and trojan horse attacks are all methods used to obtain private information that defraud web users. The first two methods direct web users to false websites – either via an email request for information or automatically redirecting web traffic by corrupting a victim's computer. In both cases the victim thinks they are using a secure site when in fact their details are being stolen by a third party.

***“Charities have become targets because of the value of online financial transactions they now host and the amount of individuals' private data they have captured for research and marketing purposes.”***

Spoof charity emails and websites like this often appear during international appeals in the wake of significant natural disasters such as the 2004 Asian tsunami and Hurricane Katrina in 2005 when the public's desire to act quickly is taken advantage of.

Trojan horse crimes are more sophisticated as they take over the



*In the murky world of criminal attacks on people's computers communication of a one-time password on a mobile phone via a text message has many advantages.*

user's entire PC. This happens when corrupted files – which appear to be useful and innocent programmes like a screensaver or game – are downloaded by the user in good faith but then execute a malicious code that gives the fraudster complete control over a PC while it still displays information the user expects to see.

***“Trojan horse crimes are more sophisticated as they take over the user's entire PC.”***

Both pharming and trojan horses can be used to deploy “man-in-the-middle” attacks where a third party intercepts a legitimate exchange and can modify information in real time before passing it on to its intended recipient. For example, in an online donation scenario, details such as where a payment should be sent and how much should be paid could be changed with neither the giver nor the recipient aware of anything untoward.

**FIGHTING THE FRAUDSTERS.** Such attacks will no doubt become

increasingly commonplace and aggressive as charities expand their online activity further and fraudsters decipher more sensitive information to maximise the impact of the crime committed. As a result, it is becoming difficult for charities both to be sure about a website user's identity and, at the same time, for users to have the confidence that they are communicating with an authentic website.

In light of this, organisations in the third sector have a real need to control access and protect the identity of users in a way that applies the simplicity of traditional “name and password” solutions but introduces an additional layer of personalised security. This must take into account a number of factors including effectiveness against known and foreseen threats, the cost and ease of implementation, flexibility and how easy it is for end users to understand and employ the technology.

#### **authenticating**

**A TWO-FACTOR APPROACH.** Although different approaches have been developed, authenticating a user based on what they have and what they know is becoming the accepted security benchmark. This has led to a significant increase in the acceptance and deployment of two-factor authentication (2FA) solutions as a means to control access to web applications and provide additional protection of user identities.

***“...it is becoming difficult for charities both to be sure about a website user's identity and, at the same time, for users to have the confidence that they are communicating with an authentic website.”***

2FA is characterised by the fact that the user knows something – such as a password or a passphrase – and possesses something which is hard to steal or counterfeit, and which provides additional identification.

In most 2FA applications “possession” is demonstrated by knowledge of a one-time password (OTP) that is generated either by a token, or at an initial login phase by the website's server, and is communicated to the end user via a device such as a mobile phone.

#### **once**

As the name suggests, this password can only be used once – in real time – to authenticate the user for the associated data or financial transaction. This negates the possibility of a “constant” password being lost or forgotten, or from being stolen via a phishing attack and then used to access a system illegally on a future occasion.

The fact that the OTP is generated by a known source, communicated by an independent medium (not via the Internet) and



*There has been a significant increase in the acceptance and deployment of two-factor authentication solutions as a means to control access to web applications and provide additional protection of user identities.*

has to be inputted by the user before an operation is verified makes it almost impossible for a man-in-the-middle attack to succeed.

Moreover, providing an additional layer of security in this way does not have to compromise anonymity – clearly an important factor for some donors and recipients. Just as a username and password does not necessarily divulge a user's real identity, so an OTP is a collection of random letters and numbers that give nothing away.

Using a mobile phone as the device on which to communicate an OTP (via a text message) has many advantages. Users are familiar with mobile phone technology and, unlike other devices such as handheld readers, the public's everyday reliance on their mobile phones means that the interface is nearly always available.

#### hardware

Another key advantage is that no additional hardware – sometimes called a "token" in this context – needs to be purchased or deployed, reducing the cost of 2FA implementation. These benefits combine to make mobile phones the preferred 2FA tool of the future.

**PROTECTING THE FUTURE.** There is little doubt that the charity

sector will continue to harness the power of the Internet to broaden communications, encourage donations via innovative online techniques, increase memberships, and keep its networks of remote workers and volunteers informed and involved at a local level.

At the same time, the sector stands to suffer doubly from the impact of financial fraud as not only does the individual charity lose out if funds are stolen via online attacks, but so too do the potential recipients who stood to benefit from the use of these same funds. Moreover, a fall in confidence amongst potential donors caused by security lapses in online giving and purchasing websites could have an additional negative impact on charity income.

***"...providing an additional layer of security...does not have to compromise anonymity – clearly an important factor for some donors and recipients."***

Hence the recent series of high profile data losses in the public sector should be a wake up call for senior managers in charities. The third sector has already started taking action with some leading organisations, including the Salvation Army and Cancer Research, joining forces to set up a specialist "security forum". Among other things, this body is looking at compliance with the Payment Card Industry Data Security Standard (PCI DSS) to help secure online credit and debit card transactions.

**LEARNING LESSONS.** Two-factor authentication can play an essential role in addressing the range of threats attracted by the potential value of data – both personal and transactional – now being shared across charity networks. Indeed, it is precisely because financial institutions are using techniques like 2FA to beef up their online security that charities are becoming more of a target in the first place.

Whilst they will never enjoy the same resources as banks, and have different priorities, the threats they face from conducting activity online are very similar. By learning from the financial sector, charities can ensure that they too take a stand against e-criminals and force them to go phishing elsewhere. ●●●