WHO'S MINDING THE (DIGITAL) STORE?

BY JOHN HAAK

The Festival business is undoubtedly a business based on fun. But if you noticed I used the word business twice in the first sentence, it's because it is a business. Most of our organizations are non-profit or Not-For-Profit entities, but I want to point out that these are tax statuses, not business goals. You do not need a plan to make gobs of money, but you do need to make enough to be sustainable. If we consider live events as a business, we need to meet the four basic tenets:

1. Increase revenue
2. Reduce costs
3. Ensure your business does 1 & 2 efficiently
4. Remain secure (a.k.a. "keep someone from stealing the store").

There are several articles based on the first two goals and a few good ones on the third. I would like to offer you some points on the last goal, "minding the store," which is often overlooked. In today's world, the bad guys have upped their game. They no longer have to hit you over the head and steal your wallet or break into your offices and drag away the safe. Hackers can take everything you have from the other side of the globe without ever leaving their seat, and since no physical harm was done, your case becomes a lower priority for law enforcement.

Like any other security briefing you've ever read, there is a scare factor inflicted by the author (me) when we say we see threats that you believe will not ever happen to you. I get it; this article is not meant to be a scare tactic, DefCon1 level, all-out alert. It is a "cautionary tale" that you might want to be looking at.
So, let's break this down. Digital threats happen in a myriad of ways but today we are going to look at four of them: Patron payments, patron information, company funds, and your marketplace. Along with providing insight into these threats, I will also discuss the simple (but not foolproof or exhaustive) protections that can be administered to make it easier for the bad guys to go somewhere else.

Patron Payments

The easy way to look at how bad actors access this information is the classic shell game: The key is misdirection. By getting search engines to point to a similar, but fake, website URL, bad actors can glean large amounts of fake ticket revenues, in addition they also get the "gift that keeps on giving", your patrons actual credit card information.

I can hear you saying, "My site is secure," so no worries, right? But what if the person / people / firm / agency who has the login to your site, or the registration to your URL, received an email from YOU asking for that login? What is your current procedure before they send out the keys to the kingdom?

Unfortunately, as the owner of a fantastic event, your name and email are fairly easy to find. And the logo of your business is virtually everywhere. If you took 10 minutes with your existing skills you could probably come up with a pretty convincing email template to send an official request from yourself. Now for the reality check: the bad guys can make any email from anywhere appear to have come from your email address (check your spam folder for how many offers came *from* you *to* you).

This misdirection happens more often than you'd think. The CEO emails an urgent check request to the bookkeeper asking that an overdue commitment that he made be wired $104,122.33 to X account–and before lunch, please. And the email actually looks like it came from the CEO, but said CEO did not send the request, and the wire went to an Eastern bloc nation with no retrieval possible. That would be terrible, but your issue would be worse: what if one of your employees received the following request: "Hey Sam, I am using XYZ Co. to do some Search Engine Optimization analysis for me, can you zing the login for the URL to me this morning please?" There goes your website … and all of your revenue, not to mention the valuable data contained within.

Would your employees respond? What if they answered like this? "Hey Jim, as we discussed, call me in person, please. We need to talk before I can send anyone anything (including you)." Set a *rule*, no one in your organization–up, down, insider, outsider–moves data or money from an email request alone. Similarly, any sensitive logins need to be changed every time someone who had access to them is no longer assigned to the task involved.

Patron Information

Data is more powerful than money; with the right access to data, you can move all the money you want. Your patrons for the most part do not trust you as an individual. If you walked up to them on the street and started asking a bunch of questions, they would probably walk away. Your patrons trust your *BRAND*, so if you did the exact same thing, but wore a big foam hat with your logo stickered on it and an apron–et voilá!–instant access.

The same thing could happen with an electronic survey. What if a bad actor sends a "Friends of the Festival" survey to all of your past patrons, requesting their Email, Facebook, Twitter, LinkedIn details? The likelihood of your patrons providing that information is pretty high. Protect your brand and your data: Know who has access to it at all times and at all points. Do you use a third-party tool to acquire and consolidate the names on your "Join the list" feature on your site?

Your ticketing company is probably your largest single collector of your patron's data; do they use it for their own purposes? Do they sell or rent your lists? When you send the list to an email engine company like Mailchimp to perform an eblast, do you send *all* the record data or just the email address alone? What is that company's policy on reuse of your names? Do ALL of your third-party suppliers also have a policy regarding answering email requests for your list? How easy is it in your organization to download the list from the server: is it in a password-protected folder and how incredibly simple is that password?

Company Funds

This was the very first fraud occurrence I was ever aware of and it was over 20 years ago. Simple invoices for copier toner were sent to large companies. The supply "company" and the "supplies" were completely fictitious. The scheme depended on the traditional large organization flaw that one department did not know what the other one was doing, so accounting paid an invoice for supplies that marketing supposedly received. Again, I can imagine that your argument is, "But our organization is small, we all communicate very well… Until the last week before the event and then things get a bit hectic and payments have to go out at a frantic pace…" You could not write a better script for a fraud scheme–Oh, wait! Yes you could! What happens if you invoice *and pay* electronically instead of using a hard (paper) invoice and the USPS to mail a check? How difficult would it be for you to call your ticketing company's accounting department and request funds to be sent to a new account? What is the established procedure to redirect millions of dollars: An email request from the right guy? A phone call from someone they have never spoken to?

Note: My day job is as a ticketing company executive in which I have a personal, direct relationship with many, but not all, of my clients. I typically see a change request email that comes into accounting, which is then forwarded to the person who manages the account on a day-to-day basis. A call would then be made to you the client (not your office, not your company, but to you, you). I would ask you if you made the request, and I would also ask you something we would both know pretty exclusively, (for example, what was the toast out on the patio at the IFEA Convention in Tucson, AZ) just to make "polite certainty." If that is all good, the change is initiated. If I do not know you well, we would still call you at your office, and request specific information that we have sent you in past payments.

So, what is the procedure with your third-party vendors if you were to change your account information?

Your Marketplace

If you owned a brick-and-mortar store, you would want it to be somewhere safe and clean for your patrons. You would want to keep the front steps free of thugs and dangerous situations and you would want to ensure the roads and services to your store were open and in good order. As of the first of this year, Google is now trying to help companies protect their brand by not allowing unassociated entities to advertise your event using misleading URLs or including artist or event names in their descriptions. It is a start, but do not trust that alone. Who on your staff is *checking for your brand every day*, including what information is available about your company or event, and what site appears at the top of the results when you do a search engine query? Do other entities use any of your keywords including your actual name? Google cannot police them all and a daily review from your team will help ensure your fans purchase from your official site.

Using the brick-and-mortar analogy again, what if the street was blocked to your store or if a street gang decided to close all access to your front door? In the digital world, that is the most common extortion play. A weak website hosting plan can open you up to a DDOS (pronounced "*Dee-Dos*") attack (distributed denial of service, for example when a hacker simultaneously directs two million hits every minute to your website) that results in perpetual gridlock; in essence, your store is closed. What happens next? A "friendly" person contacts you, saying he / she noticed your site was down and they might be able to help fix it… for a fee.

Take steps to reduce the likelihood of this happening to you. Ask your web service provider what their security systems and fire walls are and how much traffic capacity they have for situations like these. Make sure your Facebook site has all of the essential information patrons need, including a ticket sales link and relevant event information, and ensure your ticket company offers your tickets from their main site as well.

Continued on page 90

Continued from Who's Minding the (Digital) Store? page 15

A third type of attack on your marketplace is one with which you are probably more familiar: Good ole' fashioned scalping. You increased ticket purchasing convenience when you went online, but you also then made it easier for bad actors to purchase all of your inventory in a matter of seconds through the use of automated "bots" and other programs. We have all seen the CAPTCHA ("Please type the scrambled letters") screen where legitimate patrons have to decide if that is a "b" or a "6" to keep bots from cleaning us out. That is effective but has a frustration price. Consider a company that can filter the good from the bad in the background.

In Conclusion

I hope I did not scare you into going back into the stone ages and exchanging livestock for a lanyard with a rock on it as proof of purchase (rocks are hard to print on). But just like your Sheriff or Police Chief tells you every year to lock the box office door and watch for the hidden spots, be a bit more vigilant on the digital side as well. Most of these protections can be handled before you ever go on sale, so plan ahead and prioritize security and fraud prevention.

John Haak has been in the Festival and Event business for 15 years and in that time has assisted over 1500 events with their admissions and cash management needs. He has assisted some of the largest events in North America including the Indianapolis 500, Oshkosh Air Venture, the Reno Air Races and NASCAR events. John is the Director of Motorsports for Etix and is based in the Houston office.