Cultural Daily

Independent Voices, New Perspectives

Online Security for Arts & Culture Organizations

Dan Matthews · Wednesday, February 19th, 2020

Whether it's a performance of *Our Town* at a community theater or a Monet retrospective at a major metropolitan art museum, there's a chance cybercriminals want something far more valuable than the price of a ticket. Nonprofit organizations, particularly ones working in the arts and social activism, are especially vulnerable to online phishing and other cybersecurity attacks by hackers.

Nonprofit directors and IT staff need to ensure their computer systems are secure so they don't lose access to data or have private information compromised. They also need to train all staff and volunteers on how to avert stealth attacks through organization computers, such as opening emails that can direct malware into the computer system.

Attacks on Organizations

Hackers unleashed a ransomware attack on the computer system of the Asian Art Museum in San Francisco in 2019. This stopped its entire digital presence in its tracks, but the museum's IT staff was able to take back control of its system without paying the cybercriminals. Two years earlier, the Denver Art Museum also fell prey to a phishing scam, in which the personal information of 800 people who interacted with the museum, including both employees and donors alike, was hacked.

Of particular concern for museums whose data is compromised is that online databases store information on upcoming donations of art, which can lead criminals right to the where the art is currently being housed.

Other phishing schemes try to lure victims into participating in a cause that's so meaningful to them they let their guard down in monitoring for scams. For example, a December 2019 phishing scheme targeted environmental activists who found emails in their inboxes asking for support of teen climate change activist Greta Thunberg, who had just been named Time Magazine Person of the Year, and for recipients to turn out for a demonstration. The email seemed to target young people since many of the emails were sent to .edu domains. Sent in several languages, the emails told the recipients to click on an MS Word attachment. If they did so, the malware Emotet was installed on their computers.

Nonprofits on Alert

With their mission of accomplishing work for the public good often with little money, online security sometimes can take a backseat to other nonprofit priorities. A 2018 cybersecurity survey of nonprofit leaders by NTEN, an association of tech employees working in nonprofits, revealed a

range of vulnerabilities.

While 71% backup their computer systems, nearly that many lack documented policies and procedures about what to do in case of an attack. About 46% have internal policies on how data is shared outside of their organization, while the same number do not. The remaining 10% don't even know if they have these policies or not. Only 15% of the organizations have done a drill to simulate what they would do in the event of a cyberattack.

Vulnerabilities and Security Steps

It's important to know your enemy and understand what the possible threats are. In a ransomware attack, cybercriminals worm their way in through lax security and take control of your computer. There are five types of ransomware, each of which inflicts a somewhat different form of damage, which is extremely hard to undo without paying a steep price. Cryption is the most popular, and does what its name suggests — encrypts your data and holds it hostage until a ransom is paid.

Other types of ransomware include locking you out of your operating system, and scareware, which is disguised as an antivirus program that invades your computer and demands money to fix "problems." Another scheme involves leakware, which steals photos and personal information that might be embarrassing or incriminating. It then threatens to post it online, trying to blackmail users into paying up.

As art and cultural organizations continue to collect ever more vast amounts of data — everything from an inventory of their collections to their customers' credit card numbers — thieves sometimes aren't far behind in trying to breach firewalls or find vulnerable security to steal this information.

To get ahead of them, take stock of your data and all the places it's housed to get an idea of the risk that might be involved in a breach. The Federal Trade Commission recommends shoring up security in three basic ways:

1. First, security software must be installed and set to update automatically to avoid thieves finding new ways around it. Vulnerability analysts in particular might come in handy here, as they are the best way to shine light on vulnerabilities from a very real outside perspective.
2. Next, back up data and files offline so that if your system is hacked you still have access to the information elsewhere. This information and data could be housed in the cloud or on a separate server.
3. Finally, staff need to be trained on these policies and the accompanying threats, and know how to ensure they aren't exposing their organization to risks by using weak passwords or clicking on links that might unfurl malware. The NTEN survey found that only about 40% of nonprofits provide training regularly.

As cyberattacks grow more sophisticated, nonprofits have a lot to lose if their data is hacked or their computer systems are commandeered by ransomware. Nonprofits and cultural centers can be particularly vulnerable because their donors may be impassioned for a cause and let their guard down, and small nonprofit budgets sometimes don't accommodate online security protection. However, there is help and training available, and professionals who can assist on a part-time basis.

This entry was posted on Wednesday, February 19th, 2020 at 12:30 pm and is filed under Technology, Visual Art

You can follow any responses to this entry through the Comments (RSS) feed. You can skip to the end and leave a response. Pinging is currently not allowed.