Practical Digital Security for Your Gallery

By Daniel Doubrovkine

Yahoo. eBay. LinkedIn. JPMorgan Chase. The Democratic National Convention. Sony.

The number of data leaks and hacks in the last few years is staggering. And while art and design galleries may not have the type of sensitive data a presidential candidate or bank has, you certainly don’t want to have your inventory and collector data leaked or leave yourself vulnerable to malware that holds your system hostage.

Unfortunately, hackers do not need to be especially sophisticated to gain access to most people’s private information. A recent report from Verizon highlighted that 18% of reported hacks are internal—these types of hacks often result from individuals gaining access to your passwords or sensitive information through low-tech means.

Galleries may not be tech companies, but digital security savvy is quickly becoming necessary for every company with an online presence. You can make your life easier and improve your gallery’s security at the same time by taking a few simple, practical steps.

Use a Password Manager for Your Entire Life
Many galleries write down passwords on a single document and share it with the entire staff, often using the same password across multiple services. This is both inconvenient and unsafe, as a hacker could gain access to all of your data by breaking into just one of the websites.

Thankfully, password managers such as 1Password or Dashlane solve this problem in a secure and convenient way. These inexpensive services store all of your passwords in “vaults” and allow you to share specific passwords with multiple users, if desired.
For example, I share a “Family” vault with my partner, an “Engineering” vault with Artsy Engineers, and an “NYC Office” vault with all of Artsy’s New York employees. I can unlock all of these vaults with my personal “master” password that is known only to me.

Every time you or a team member signs up for a new online service, you can use your password manager of choice to generate a new unique password and add it to the appropriate vault instead of passing it around on post-its or having to remember it.

Store Everything in the Cloud
While it’s true that online service providers can be hacked, they’re in the business of keeping you safe and are constantly improving. They also offer the side benefit of being cheaper and having lower setup costs than on-premise systems, so they’re easier to try out.

Cloud applications reduce the risk of losing customer data and allow you to access your files from multiple locations, like when you’re travelling to art fairs or working from home. Your data also won’t be lost in the case of a natural disaster and you can even double-insure yourself with services like Backupify.

I recommend getting started with GMail for all your e-mail and Google Docs for documents. You may want to use Dropbox or Google Drive for artwork images or settle on a complete inventory and customer relationship management service, depending on the size of your client base.

I also tend to scan all my documents and eventually shred originals. A professional-grade printer/copier/scanner helps make this process easy by scanning and e-mailing documents in just a couple of seconds. Storing scans in Dropbox is a lot more secure than storing documents in your cabinet!
Create Personal Logins and Lock Your Computer
Whenever you use someone else's computer, make sure you either use the Guest account or create a personal login and password. Using someone else's account can be dangerous as your personal information might be saved. Once you've logged in to your password manager, you're instantly ready to be productive!

Don't forget to enable a screensaver that locks your screen and requires a password to log back in after a few minutes. It's an easy way to prevent anyone from being able to read what's on your screen when you walk away for a lunch meeting.

Create Checklists for Onboarding and Offboarding Employees
It's easy to add a new employee to services like GMail or Dropbox, but remembering to remove them is another matter.

And if the person running some or all of your Snapchat, Facebook, Twitter, and Instagram accounts leaves, you shouldn't have to scramble to find and change the passwords. If you've invested in a password manager, all you have to do is remove them from the vault. Either way, I encourage you to create checklists for onboarding and offboarding employees that cover such things as adding them to and removing them from team accounts.
Secure Your WiFi Network
A computer connected to your private WiFi network can “see” all of the computers connected to it—a simple misconfiguration or an inadvertently shared drive can leak all your information.

Ask your IT provider to set up separate WiFi networks for your internal staff with a strong password and an open WiFi or one with a simple password for gallery guests. Keep the WiFi password in a password manager shared with your team.

Educate Your Staff
Most security problems are very low tech. Teach your team to treat your gallery’s private information the same way they would treat their own bank account logins and passwords. This includes never writing down passwords or reading them loud, deleting suspicious emails, and never opening questionable attachments that could contain viruses.

Stay safe!