artnet news

May 24, 2024

‘The Scams Keep Proliferating’: Christie’s Historic Outage Reveals the Art World’s Digital Vulnerabilities

The bad guys’ tools range from good, old-fashioned fraudulent checks to the most advanced technologies.

By Brian Boucher

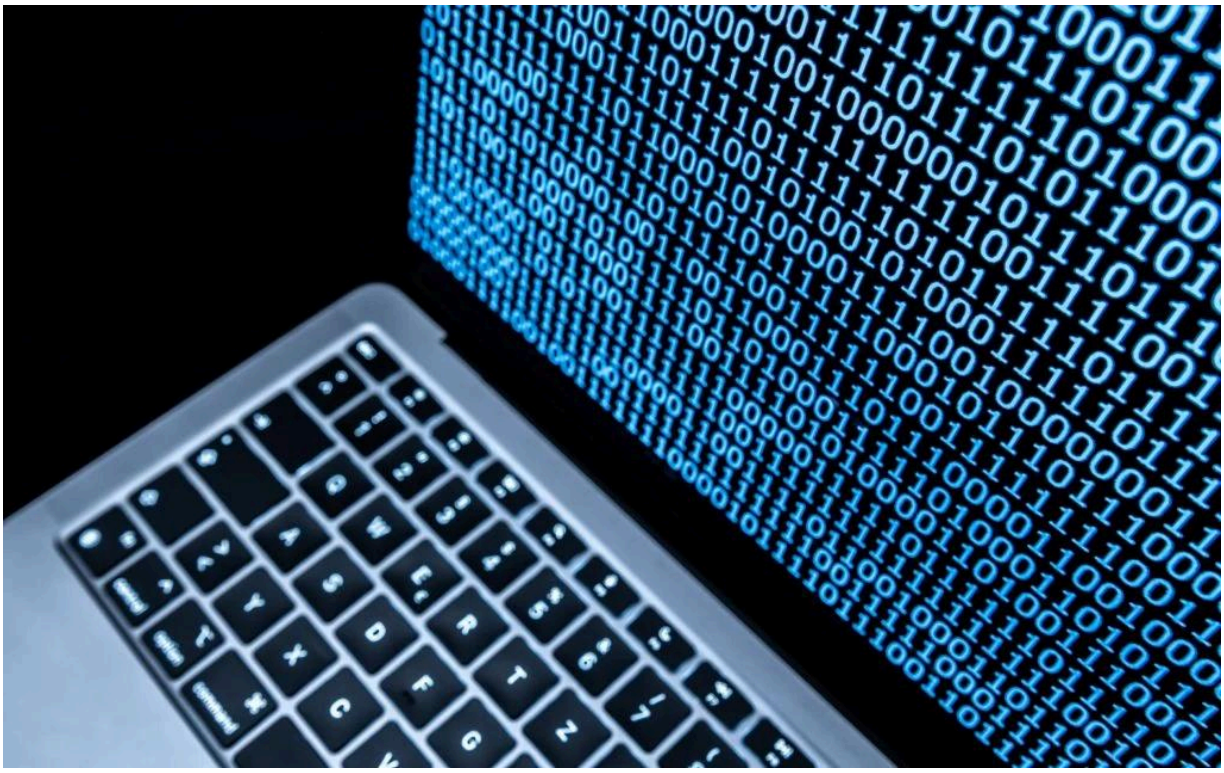


Photo: Silas Stein/picture alliance via Getty Images/

Christie’s may have breathed an enormous sigh of relief on Saturday evening when, after nine days, its website and app were restored to full functionality following what the house would only call an “incident” but is widely understood to have been an unprecedented hack or ransomware attack.

The “incident” revealed that even the art world’s largest businesses are vulnerable to bad actors, and that the price could be steep: *Vanity Fair*’s Nate Freeman reported that according to one rumor, the hackers were demanding a ransom of $20 million.

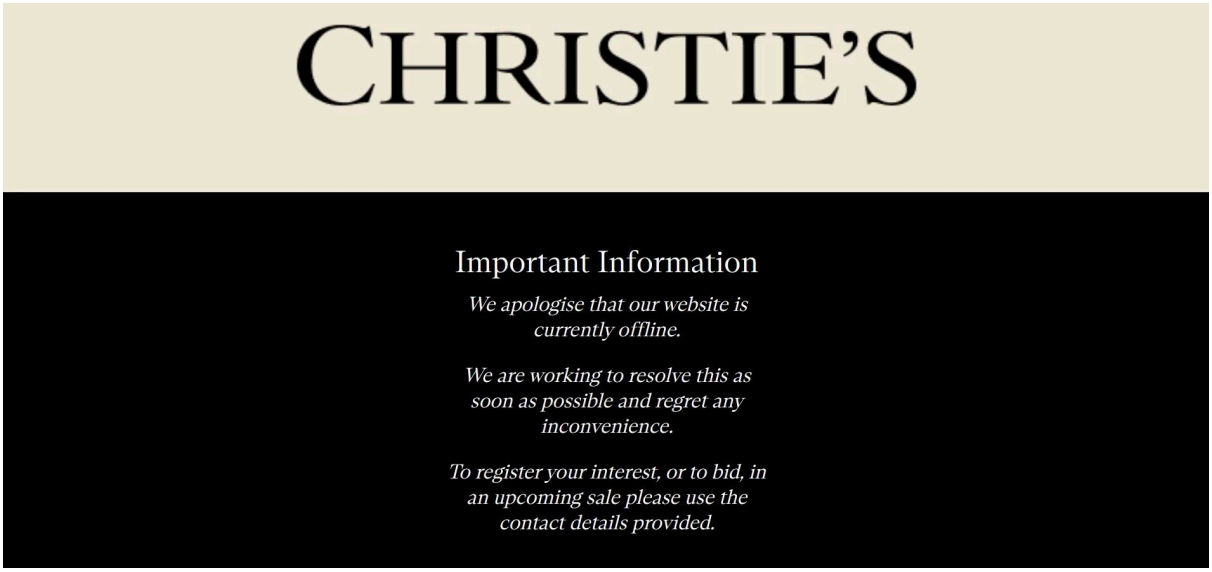
Christie’s declined to provide any specifics about the incident. “Our investigation into this incident is ongoing,” said a spokesperson, “and therefore we are not able to share any further information on this for the moment.” Another major international auction house would say only that it takes these matters

extremely seriously and that it proactively runs regular tests to ensure that systems are secure; others did not reply to requests for comment.

But Christine Plaggemier, executive director of the nonprofit National Cybersecurity Alliance, was willing to offer some surmises about the situation.

“When an organization remains offline for an extended period, as Christie’s did, it often indicates a ransomware attack, suggesting they are not paying the ransom, which is a commendable decision,” Plaggemier said on a Zoom call. “The more frequently ransoms are paid, the more incentivized criminals become.” When companies come back online quickly, it likely means they paid a ransom, and she noted that the money can be put to terrible uses: a White House official indicated in 2023 that about half of North Korea’s missile program has been funded in this way.

“Christie’s implemented a backup plan, indicating they have engaged in tabletop exercises, where scenarios of ransomware attacks or data leaks are simulated,” she said. “This practice helps organizations identify and address their vulnerabilities.”



A screenshot shows the Christie’s website down.

But what about businesses that don’t stage such elaborate exercises? If one of the industry’s largest businesses, founded in 1766 and having notched some $6.2 billion in sales in 2022, could be so dramatically victimized, what could be the fate of smaller art galleries and auction houses that may not have the same cybersecurity provisions in place, even though they may have information on wealthy clients in their files in the cloud?

“The digital scams just keep proliferating day after day,” said one New York dealer. “Not a week goes by that my staff and I don’t sit around looking at emails and saying, ‘Is this real or fake?’ Most of the fraudulent ones are evident but there are many that almost pass the smell test because they don’t have all the spelling errors you usually associate with scammers.

“I think most businesses in the art world feel Christie’s pain,” added the dealer.

A Variety of Threats, and Many Defenses

The threats businesses face are manifold. Some are as simple as good old check fraud: checks are intercepted in transit, then "washed" of the written parts, and made out to a fake account set up by fraudsters. But even those classics now have a cyber edge: distressingly, the crooks then sell copies of the checks online to other fraudsters.

According to the United States Postal Service, nearly 300,000 mail theft complaints were filed in the first year of the pandemic, up some 161 percent from the year before. The *New York Times* reported that "financial institutions also reported triple-digit increases." In its defense, the USPS said that postal inspectors recover more than $1 billion in counterfeit checks and money orders annually.

And, of course, while the days of paper checks are on the wane as business has largely moved online, old scams have been replaced by cyberthreats of all sorts. The Federal Bureau of Investigation's Internet Crime Complaint Center indicated that losses in this realm mounted from $2.7 billion in 2018 to $10.3 billion in 2022. The National Cybersecurity Alliance, meanwhile, indicated that globally, cybercrime is projected to cost $10.5 trillion annually by 2025.

As there are many threats, there are numerous protective steps businesses can take.

The Art Dealers Association of America (ADAA), a nonprofit organization that serves over 200 galleries, is very much on the case, offering members a variety of resources, including a members' seminar led by an agent from the FBI's Financial Cyber Crimes Task Force.

An image of a seized ransomware website is displayed at an FBI press conference. Photo: Kevin Dietsch/Getty Images.

“The bad actors have gotten a lot more sophisticated,” said ADAA executive director Maureen Bray. Among the major scams dealers face, she said, are the “man in the middle” scheme, in which criminals monitor a business’ emails, contact the recipients of invoices, and, closely mimicking the sender’s language, ask that the recipient direct the payment to a different bank account. (The *Times* reported that there may be as many as 2.5 million fake accounts worldwide set up for these “nefarious dealings.”) For a time, especially when so much business went online during the height of the pandemic, Bray noted, the trend was hackers taking control of galleries’ Instagram accounts and holding them for ransom.

“You’re vulnerable in the analog world *and* in the digital world,” Bray said, “but using one to protect the other is the safest bet.” She tirelessly urges member galleries to adopt multi-factor authentication, including sending password-protected invoices or only confirming bank details via phone.

She acknowledged that proper protections can be time-consuming. “But,” she said, “it takes a heck of a lot more time and energy to repair the damage than it does to be proactively secure.”

The combination of high-tech communication and being pulled in numerous directions at once makes businesses highly vulnerable, Bray pointed out.

“The problem is partly the speed at which we exist,” she said. “You’re in the back of a cab looking at an email on your phone and you’re more likely to click on a link because you didn’t read it carefully. They know your attention is divided, and this is fertile soil for bad actors.”

‘Devastating and Insidious and Brilliant’

One American art dealer told a harrowing tale on condition of anonymity to avoid being re-targeted. As the dealer explained: “It’s not just one and done. The experience goes on and on, the way these thieves operate. It’s devastating and insidious and brilliant in a way.”

It all started in January when the dealer, checking their bank account, saw a large outgoing check that was not sent by the gallery; the fraudulent check, on close inspection, was a handmade reproduction of the business’ checks. Meanwhile, some checks sent to artists had never arrived. “Since then,” they said, “we have gone completely check-less. Unless I’m handing it to the recipient, no paper checks.”

But that wasn’t the end of it.

“A second check then popped up for an even more eye-watering amount—six figures debited from our account. And simultaneously, we received an onslaught of robocalls, phony texts, and spam emails. Every point of entry for communication was clogged. The reason, which was not apparent at first, was that somewhere in there was one important message saying that someone had contacted our bank to change our password.”

And, said the dealer, don’t count on even the largest bank to help: “Chase was miserable at first in helping us deal with this.” The dealer had to personallywrite to Chase’s CEO, Jamie Dimon, to get swift assistance.

The dealer has set up more than one measure to avoid any further scams.

“Every check we write now has to be approved online in a secondary measure,” they said. “We have the same protocol in place for ACH transfers or deductions from the account. Each time one comes up, we

get a text and an email alerting us and we have to approve the transaction. It gives us an extra measure of safety."

Plaggemier noted that art dealers may face particular challenges. "For the average art dealer," she said, "there is money changing hands with artists and customers, so there are a lot of moving pieces and a lot of opportunities for money to get into the wrong hands. And it's getting harder and harder to recognize what's malicious and what's not."

Cloudy Skies Ahead?

Galleries count not only on their banks but also on the systems that store information in the cloud. Artlogic is an online platform that provides inventory, sales, website, and marketing functionality to some 12,000 art world clients. As many as 10 million artworks have been stored, managed, shared, and sold on its platform, and its clients include galleries such as Victoria Miro, Thaddaeus Ropac, Esther Schipper, P.P.O.W, and Jessica Silverman. An outage at a centralized company like this could pose a serious threat to galleries that rely on it.

"Security has always been paramount in the art world and even more so in today's landscape where galleries have been actively transitioning from using on-premise software to online-first solutions," said Artlogic CEO Mike Profit. "Art businesses can protect themselves from cyber threats—which could range from data leaks to payment fraud—through partnering with trusted providers and having a robust response plan in place to prepare organizations against attacks."

Plaggemier of the National Cybersecurity Alliance stressed that businesses have to take important steps against widespread threats—and right now.

"The vast majority of these attacks start with a phishing email—I've read as much as 92 percent to 98 percent," she said. "If you're not training your employees and sending fake phishing emails to test them, you're behind the times."

The newest technologies will make the problem even worse, she said, especially A.I. and the deepfakes it allows.

"It's going to get worse and worse," she said. "We've heard reports of people being on calls just like this one, but they were talking to the bad guys. You're seeing their face and hearing their voice, but it's being controlled by a puppet master."

And, she pointed out, attacks don't need to be high-tech to be damaging.

"I've got sophisticated, educated businessmen who fell for romance scams on dating apps," she said. "This truly can happen to anyone."