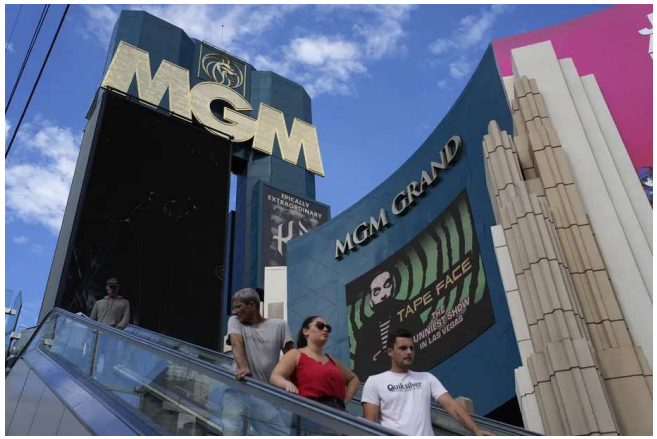
TECHNOLOGY CYBERSECURITY PRIVACY & SECURITY

The chaotic and cinematic MGM casino hack, explained

A “limited number” of customers’ Social Security numbers were taken.

By Sara Morrison | sara@vox.com | Updated Oct 6, 2023, 11:25am EDT



People riding an escalator outside the MGM Grand in Las Vegas. Unlike some parts of MGM’s business that were affected by

Most Read

1 Why did Hamas invade Israel?

2 This Gaza war didn’t come out of nowhere

3 What are Israel and Palestine? Why are they fighting?

4 Benjamin Netanyahu failed Israel

5 What a “complete siege” of Gaza will mean for Palestinians

the hack, the escalators remained operational. | AP/John Locher

Sara Morrison is a senior Vox reporter who has covered data privacy, antitrust, and Big Tech's power over us all for the site since 2019.

Did prominent casino chain MGM Resorts gamble with its customers' data? That's a question a lot of those customers are probably asking themselves after a cyberattack took down many of MGM's systems for several days. And it may have all started with a phone call, if reports citing the hackers themselves are to be believed.

MGM, which owns more than two dozen hotel and casino locations around the world as well as an online sports betting arm, **reported** on September 11 that a "cybersecurity issue" was affecting some of its systems, which it shut down to "protect our systems and data." For the next several days, reports said everything from **hotel room digital keys to slot machines** weren't working. Even websites for its many properties went offline for a while. Guests found themselves waiting in hours-long lines to check in and get physical room keys or getting handwritten receipts for casino winnings as the company went into **manual mode** to stay as operational as possible. MGM Resorts didn't respond to a request for comment, and has only posted vague references to a "cybersecurity issue" on Twitter/X, **reassuring guests** it was working to resolve the issue and that its resorts were **staying open**.

It took about 10 days, but MGM announced on September 20 that its hotels and casinos were "operating normally" again, although there may be some "intermittent issues" and MGM Rewards may not be available.

"We thank you for your patience," the company said in **its statement**. It did not provide any additional information on the reason why its systems went down in the first place.

Several weeks later, on October 5, MGM provided another update with some bad news for its guests: The hackers were able to access their personal information, including names, contact information, gender, date of birth, and driver's license, passport, and even Social Security numbers, from "some customers" before March 2019. The company did not reveal just how many people that includes, but says it is providing free credit monitoring services to them, which has become the **standard response** from companies who can't secure their customers' data.

The attacks show how even organizations that you might expect to be especially locked down and protected from cybersecurity attacks — say, massive casino chains that pull in tens of millions of dollars every day — are still vulnerable if the hacker uses the right attack vector. And that's almost always a human being and human nature. In this case, it appears that publicly

available information and a persuasive phone manner were enough to give the hackers all they needed to get into MGM's systems and create what is likely to be some very expensive havoc that will hurt both the resort chain and many of its guests.

Spiders and Cats are claiming responsibility for the attack

A group known as **Scattered Spider** is believed to be responsible for the MGM breach, and it reportedly used **ransomware** made by **ALPHV, or BlackCat**, a **ransomware-as-a-service** operation. Scattered Spider specializes in **social engineering**, where attackers manipulate victims into performing certain actions by impersonating people or organizations the victim has a relationship with. The hackers are said to be especially good at "vishing," or gaining access to systems through a convincing phone call rather than phishing, which is done through an email.

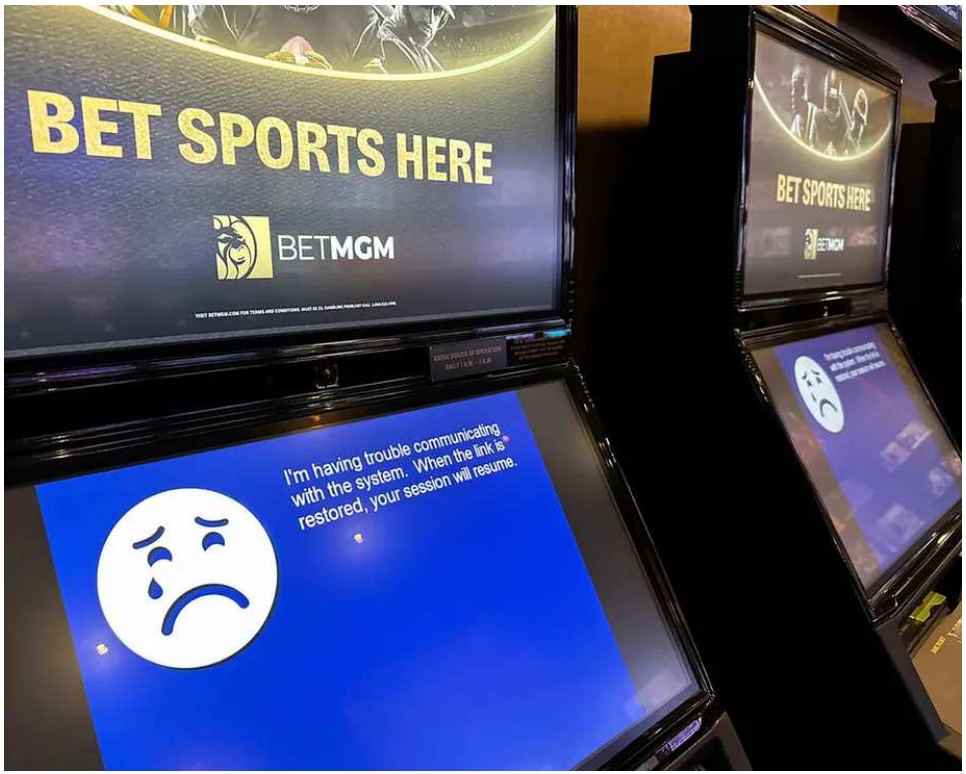
Scattered Spider's members are thought to be in their late teens and early 20s, based in Europe and possibly the US, and fluent in English — which makes their vishing attempts much more convincing than, say, a call from someone with a Russian accent and only a working knowledge of English. In this case, it appears that the hackers found an employee's information **on LinkedIn** and impersonated them in a call to MGM's **IT help desk** to obtain credentials to access and infect the systems. A **subsequent Bloomberg report**, citing an executive at cybersecurity company Okta, blamed a successful social engineering attack on the help desk as well. MGM is a client of Okta's and the company has been assisting MGM in the wake of the attack, the report said.

Someone claiming to be a representative of Scattered Spider **told the Financial Times** that it stole and encrypted MGM's data and is demanding a payment in crypto to release it. This was the backup plan; the group initially planned to hack the company's slot machines but weren't able to, the representative claimed.

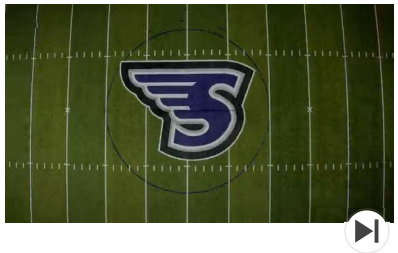
If that all has you thinking that we're in the middle of a remake of *Ocean's 13*, you should also know that it may not be accurate. ALPHV/BlackCat is **denying** parts of these reports, especially the slot machine hacking attempt. The group posted a message on September 14 claiming responsibility for the attack but denying that it was perpetrated by teenagers in the US and Europe or that anyone tried to tamper with slot machines. It **also criticized** what it said was inaccurate reporting on the hack and said it hadn't officially spoken to anyone about the hack, and "most likely" wouldn't in the future. The message said that data was stolen from MGM, which has thus far refused to engage with the hackers or pay any kind of ransom.

It seems that MGM wasn't the only casino chain hit by a recent cyberattack. Caesars Entertainment **paid millions of dollars** to hackers who breached its systems around the same time as MGM and was able to continue operations as normal. Caesars admitted to the breach **in a filing** with the Securities and Exchange Commission on September 14, where it said an "outsourced IT support vendor" was the victim of a "social engineering attack" that resulted in

sensitive data about members of its customer loyalty program being stolen. Though the method is very similar to those reportedly used by Scattered Spider and the attack happened at nearly the same time as MGM's, the alleged representative of the group told the Financial Times that it wasn't behind it. Although, again, another group seems to be denying that Scattered Spider did any of the attacks, or at least how the events have been reported isn't accurate.



A betting kiosk at MGM Grand on September 12, two days into the hack that shut down many of MGM's systems. | K.M. Cannon/Las Vegas Review-Journal/Tribune News Service via Getty Images



Why vishing works

Though we don't yet have confirmation of who attacked MGM or even how, the alleged method, vishing, is a known cybersecurity threat that many organizations haven't sufficiently protected themselves from. A portmanteau of "voice" and "phishing," vishing, like all social engineering techniques, targets what's usually the weakest link in the cybersecurity chain: **us**. More than **90 percent** of cyberattacks start with phishing, and it's one of the most common ways that organizations are penetrated as well. And vishing is a particularly effective avenue of

attack: A **2022 IBM report** found that targeted phishing attacks that included phone calls were three times more effective than those that didn't.

yet, but we may well see a lot more.

"What we're seeing, especially in the new age of **artificial intelligence**, is the attackers are leveraging not only hacked information that they find about you, but also all of your social profile information," Nicoletti said.

Stephanie Carruthers, who is a "chief people hacker" for IBM, uses social engineering to test client organizations' systems to find potential vulnerabilities. That includes vishing, which gives her a front-row seat on how it can be used to gain access to a target.

"From the attacker point of view, vishing is easy," she told Vox. "With phishing, I have to set up infrastructure, I have to craft an email and do all these extra technical things. But with vishing … it's picking up the phone and calling someone and asking for a password reset. It's pretty simple."

One of the keys to a successful vishing attack is knowing enough about a system, company, or employee to pull off the impersonation. You can learn a lot about people and organizations just from what's publicly available — including who companies' high-value targets are.

"It makes the job of an attacker so much easier," Carruthers said. "Things like **LinkedIn** and different types of people search engines, that is the first step into making a successful vish." From there, the attacker can use other **social engineering techniques** like adding a sense of authority or urgency to a request. Organizations with inadequate verification processes to prove that the caller is who they claim to be are especially vulnerable. "It's something we see happen all the time," Carruthers added.

It doesn't help that companies often overlook vishing in their employee cybersecurity training, and they aren't asking people like Carruthers to test for vishing vulnerabilities, as they do for phishing. A highly publicized attack like MGM's might change that. But it may also lead to an increase in vishing attacks, now that other hackers see that it gets results.

So what can you do to protect yourself? When it comes to attempts to vish you personally, the same general rules about being careful what information you share and with whom apply. Don't

give out your login credentials and passwords, and be careful about your publicly available data as well, since attacks may use it against you (or to impersonate you to trick someone else). Verify that people are who they claim to be before engaging with them. Use different passwords across all of your accounts, so that if someone gets access to one of them, they aren't then able to get into others, and use **multi-factor authentication** for another layer of protection.

In this case, however, there's not much people can do when a company they trusted with their data didn't have sufficient systems in place to protect it — which **a lot of them don't**. But they can do a few things after the fact to minimize any possible damage. MGM says it is informing customers whose data was stolen and offering them free identity protection and credit monitoring, but you might not want to rely wholly on a company that didn't protect your data in the first place.

Nicoletti says MGM customers should check their bank statements in case their debit card numbers were exposed in the breach, if not ask their bank for a new card entirely. He also says MGM customers should be especially wary of emails claiming to be from MGM, in case the hackers obtained customers' email addresses. And definitely don't click on any links or provide any credentials if asked.

Carruthers recommends that MGM customers be on the lookout for weird charges to their credit cards. She also recommends that they consider **freezing their credit**, which is free and easy to do and prevents would-be identity thieves from taking out credit cards in their names.

Update, October 6, 11:25 am ET: *This story was originally published September 15 and has been updated multiple times, most recently with the news that MGM is confirming that customer data was stolen.*