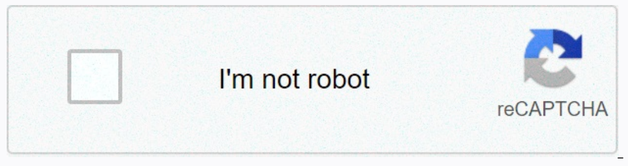

Continue

E aadhar card by enrollment number

Vendors ComputerHQ.com exposed debit addresses, credit card numbers, and other personal information using a JavaScript bug that was loaded over the weekend, a privacy expert claimed. As of Monday morning, the security breach was full. Before that, about 15,000 personal records were available to view online, according to Keith Little, an independent privacy consultant. ZD Internet/ExtremeTech verified the information with actual cardholders, who confirmed that they did make the specified purchases. Essentially, some or all of ComputerHQ.com's invoices were available to the Internet as a whole, including names, addresses, phone numbers, credit card numbers and expiration dates, as well as the products ordered and their price. Executives ComputerHQ.com, based in Fremont, California, did not reply to repeated phone calls seeking comment. A sales worker said that IT concerns had been addressed by off-site internet staff who worked for the company, and who were int answering questions. However, he said that the website was redesigned a month ago. The glitch was relatively simple, Little said: Usually, if the viewer wanted to check an order, they could visit the company's webpage, enter their order number and zip code, and a dynamically generated webpage would list the appropriate information. If he can't list his zip code, a pop-up window appears asking for focus. However, this tracking system will only work if a user's client browser was JavaScript enabled. Little said that if JavaScript was turned off, the company database was exposed to public view, one record at a time. A malicious user can simply change the order number in the URL to obtain new records. It all started the Saturday before noon, Little said. They accidentally sent me a hard drive that (my client) didn't need. On each invoice, Little said, there was a URL to check the order status using the unique order number. Little need to know the zip codes used in other orders; Instead, it can enter a URL with a similar order number and use JavaScript utilization to obtain the database information. Little said then that he called the company on Saturday, and the site was immediately taken to fix the hole. On Sunday, however, the site reappeared with the same hole, and Little again successfully requested that the site be taken. The scenario was repeated early Monday morning. This morning he was the site up and running while he made the change, Little said. No firewall, nothing. It was the dog's breakfast. Little said that, according to his call, the owner of the site apparently did its own IT maintenance and programming. The orders date back about 11 months, a time when these numbers were likely, but uncertain, that these numbers were visible to someone taking advantage of the JavaScript bug. If that didn't happen, it's a miracle, Little said. Customer reactions ranged from the angry to the patalists. I'll never... Internet businesses will ever again if those numbers can be published that way, said Shelly Tighe of River Vale, N.J., in a message left with ExtremeTech.Some customers, like Doug Burt of Newton, Massachusetts, said they got lucky, as they weren't even sure the tickets were still active. Others said they had problems with fake credit card charges, but didn't know if they were related to ComputerHQ.com Red Bank. Although some people may actively exploit weaknesses in security firewalls through active attacks, passive holes can also be common. I've seen methods proven where SQL was used with a browser, for example, to reveal database content far beyond the site operator's intent, Little wrote in a follow-up email. Ironically, one of the victims was Jeffrey Miles, an employee of Daimler Chrysler, who did work as a network privacy consultant for small businesses. I know how this can happen; It just sucks that it happened to me, miles said. Credit card numbers each serve a specific function that determines how each transaction is routed and mousses security. You probably know your credit card numbers by heart, either in full or in the last four digits. But, if you're like most people, you probably have no idea what they mean. Each has a specific identification function for your bank, system, or for you personally. While it's not necessary you know what the numbers mean, understanding the process your information goes through with any credit card transaction is still food-thought. Unlike other account numbers, like those of the gas company or phone or even department stores, credit cards all use the same number system. In this system, the number and structure of the numbers on the card indicate what type of card it belongs to. The first number on your credit card is called the Primary Industry Identifier (MII) and indicates the system to which your card belongs. Number 3 indicates American Express number 4 indicates visa number 5 indicates MasterCard number 6 indicates a Discovery credit card within each card system is a unique structure for that credit card company. For example: on American Express cards, the third and fourth digits are the type and currency, the fifth to 11th digit is the account number, the 12th to 14th digits are the number of cards within that particular account, and the 15th digit is the check number. Visa uses digits two through six for the bank number, the seventh to 12th or 15th digit is the account number, and the number 13 or 16 is the validator number. MasterCard uses digits two through six as account numbers depending on the length of it can be digits two and three or two to four or two to five or six. After the bank number, the digits that follow up to the 15th are the account number and the 16th digit is the validator number. Although it's more important Knowing where you spend your money confirms the function of your credit card numbers, it is helpful to understand the complexity of the credit card system. Once you realize how much effort has gone to ensure security and efficiency you will have more appreciation for your card. If you're looking for a new card, be sure to compare your credit card options to find the best ones for your wallet. A merchant account number for credit cards is part of a package that allows your business to take payments by processing credit card transactions. The merchant number ensures that your merchant services company will apply the payments you process through your credit card terminal to the correct account. The number appears in every credit card receipt you provide for your customers, allowing them to track and identify traffic in case of ready difficulty. Many financial institutions are vying for the opportunity to be your merchant services company. You can start choosing between them based on price. Fees vary considerably, and include charges per item, charges per month, and percentage fees in your total sales volume. Value If your business will become a larger number of small sales or a smaller number of large sales, and select a merchant service company that offers good value for your business's specific sales patterns. Before based on a company, consider other variables that might influence your decision, such as whether a company requires an extended contract, and whether you might find it simpler to work with your bank even if it's more expensive than other options. After you contact the company you decide to use, they'll make an appointment for you to see a representative. They'll bring you a request. Fill out the paperwork they provide and send all additional support materials they need, such as a blank check or revocation authorization for a credit check or criminal background check. After the financial institution approves your request, it will send a representative to help you set up your system, or send the materials to you. Your merchant account number will appear in the introductory materials you receive. You can also find it on the receipts you print and your monthly report. Contact your company's helpline if you have any questions or concerns. When Amazon packages began appearing on Chris' doorstep in Connecticut last fall, he and his wife assumed the other was buying Christmas presents for a second time. But the contents of the packages didn't look like gifts any of them would want to receive. I opened some boxes addressed to me and found some items I really couldn't identify, he said. I still don't even know what they are. There were no unnecessary orders on the couple's Amazon Prime account. When he contacted Amazon, they said he could throw away the items. He counted six packages, containing 10 or 12 items in total. The one he shared with me turned out Be a heat-powered fan for a wood-burning stove, which retails for between $45 and $55 on Amazon. Chris doesn't have a wood-burning stove. Eventually, Chris found evidence of instructions: they were into his credit card account. Someone got his credit card number and used it to book orders. And then they sent them to... Well, he is. It's a scam that doesn't make sense at first glance. Why would someone steal your credit card information just to order items they can't even use? But it's a little more complicated than that. Chris said that when he contacted American Express, his credit card issuer, they were able to help him put some puzzle pieces together: scammers access old, expired credit card numbers, then check them on Amazon to see if they were still working. Eventually, they make bigger purchases, send them to your address, and send a balcony pirate to pick up the shipment before you can spot it. While he has no proof the hack came from his Amazon account, Chris did not have old credit card numbers stored in his account, which American Express advised him to remove. It's a disgustingly clever crime, said consumer expert Clark Howard. Chris' experience seems like a na meaner version of so-called brushing. This is where third-party Amazon sellers try to boost their ratings and send their product to random people; They can then leave reviews for a verified purchase. (For more information about programs to boost the ranking of third-party sellers on Amazon, listen to the Reply All Magic Shop episode.) But the low-level flight doesn't explain how Chris' credit card number was stolen. Say you have an Amazon account for 10 years, and during that time you added five or six different payment options to your account. These cards, even if expired, can be used against you if your account is compromised. That's because credit cards like to play nice with their retail customers. If a merchant (like Amazon, for example) has an arrangement with a card issuer (like American Express) and agrees to take on the risk, they can get the green light to run cards that are no longer technically considered valid, Howard explained. The system is awake knowing there will be a certain amount of fraud, he said. But compare this small amount of risk to the amount of revenue a website can bring in by allowing purchases from customers who have forgotten to update their payment information, and it's clear why a merchant will take the risk. The only retailers unlikely to bear this responsibility are electronics stores, Howard noted. But people who engage in online fraud usually know which retailers are willing to bear the risk, like Amazon, and who won't, Howard said. As soon as we can find a card that works, it orders in your name, follows it all the way. Once it gets dropped on your porch, the crook or one of their friends can wander past to pick it up. It seems that Chris's scammers weren't so good -- either, they-- Satisfied with the individual check orders they made enough to switch to bigger and better attempts on his credit card. Shortly before Christmas, we were able to connect Chris to an Amazon team that said he would investigate, but they didn't respond to post-holiday follow-up messages. An Amazon spokesperson said in an email: We are investigating this customer's investigation into unsolicited packages because it would violate our policy. We remove sellers in violation of this policy, wither payments and process with law enforcement to take appropriate action. Meanwhile, Howard offered some tips for preventing this scenario. Select one Credit CardFirst, he recommends choosing only one credit card and one credit card for making purchases online. It's easier to track your online purchases if they're all on one card, and any suspicious activity will stick more easily. You may miss out on some rewards, but Howard says the diminished chance of fraud streamlining your activity is worth it. The next time you enter the designated card information to make a purchase, delete any other cards saved to your online account. Use one-time card numbers a second, if you want to be even more careful, is to consider using a program that provides one-time credit card numbers every time you shop online. Even if the number is compromised, it will be useless to cheat after your initial use. Your bank or credit card issuer might call it a virtual card or a virtual card number. You'll lose convenience by remembering your payment information, but you'll get financial security. Think home security at last, think about getting a camera for your front door or wherever packages stay. It doesn't have to be a smart doorbell expensive and scary; There are security cameras that cost less than $50 that can help you capture evidence of a suspected pirate on the balcony. And that evidence could help law enforcement catch thieves and crooks in your area. If something is wrong, speak quickly if you suspect you've already been flagged by a hacker who leaves gifts at your doorstep, it's essential to act as quickly as possible. If you notice suspicious account activity more than a week or two after it occurs, Howard warns that it may be harder for you to prove that you're not guilty, and that the activity is actually fraudulent. So many people never open their statements, or they don't look at their electronic statements, he said. Contact your card issuer and retailer as soon as you notice something off. While American Express could not comment on Chris' particular experience, a spokesperson sent a statement calling on consumers to protect their financial information. If they are ever unsafe, they should call their financial institution directly, the spokesman said. We will take the appropriate action immediately if we determine that this is indeed a fraud. Howard recommends initiating an online chat to let the retailer know you've received mysterious packages I have a record of your conversation. The retailer may tell you to throw away the items, as Amazon told Chris; He may request that you send the item back with a prepaid return label. Once you clean up the mess, don't let down your defenses. Once you're a sign, it's probably not going to be the only time they try to hit you, Howard warned. And the way scammers infiltrate our financial lives continues to evolve. That will continue to change, he said. Criminals continually seek weaknesses in our personal behaviors or organizational systems. The best advice in six months could be completely different because scammers have found a different weak spot. People won't notice until something happens to them. Privacy.