

# Amazon's customer service backdoor



Eric

Follow

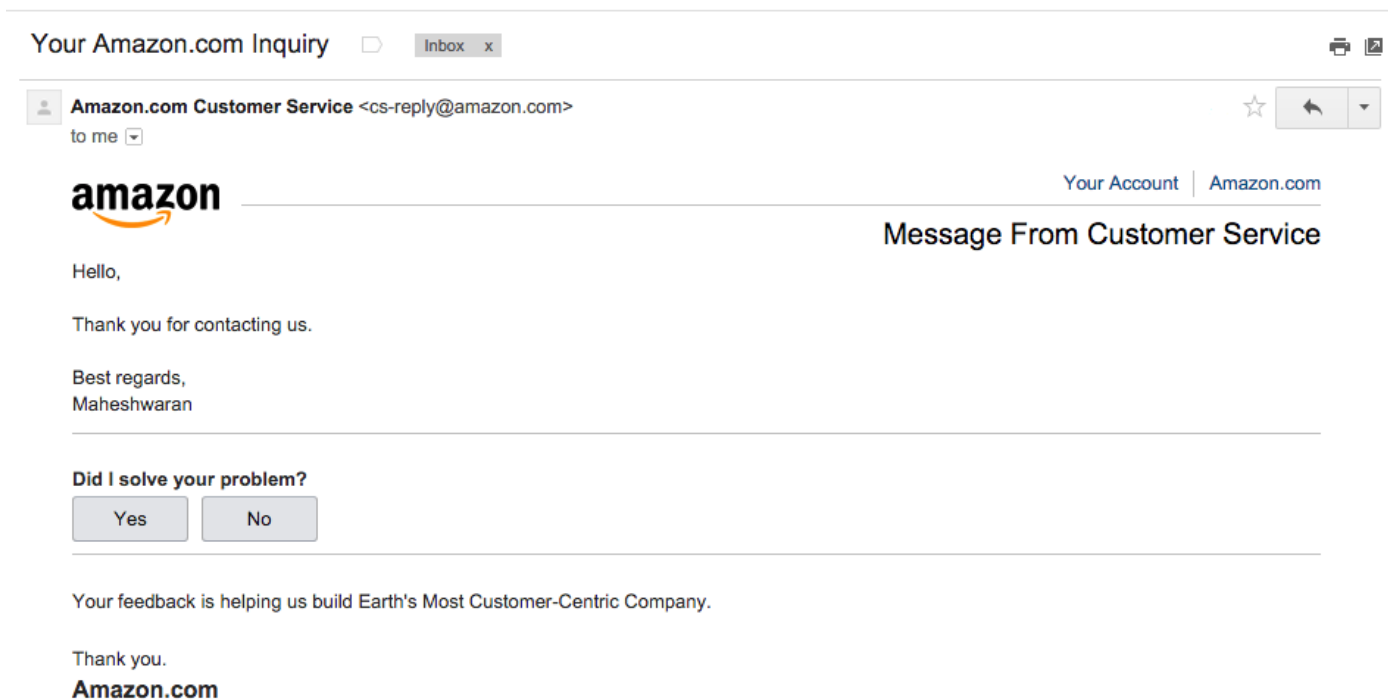
Jan 24, 2016 · 5 min read

As a security conscious user who follows the best practices like: using unique passwords, 2FA, only using a secure computer and being able to spot phishing attacks from a mile away, I would have thought my accounts and details would be pretty safe? Wrong.

Because when someone has gone after me, it all goes for nothing. That's because most systems come with a backdoor, customer support. In this post I'm going to focus on the most grievous offender: Amazon.com

Amazon.com was one of the few companies I trusted with my personal information. After all, I shop there, I used to work as a Software Developer and I am a heavy AWS user (raking up well over \$600/month)

It all began with a rather innocuous email:



Weird, I didn't contact Amazon support?

At first, I assumed it might be a mistake or a delayed email from the time I contacted them months earlier. But curiosity got the better of me, and I contacted Amazon to ask what it was about. They told me that “I” had a conversation with Amazon support? What the hell? It was a text-chat, and they emailed me a transcript:





## Message From Customer Service

Hello,

Here's a copy of the chat transcript you requested:

-----

6:40 PM Mahesh has accepted the chat.  
6:40 PM Mahesh (CSA) : Hello, Eric. My name is Mahesh. I'm here to help you today.  
6:40 PM Mahesh (CSA) : May I know your issue in detail?  
6:41 PM Eric Springer : I need to know where my latest order is being shipped  
6:41 PM Mahesh (CSA) : Let me check that for you.  
6:42 PM Mahesh (CSA) : Before that, I need to verify your account. Can you please confirm the name on your account, your e-mail address, and your complete billing address?  
6:42 PM Eric Springer : Name: Eric Springer  
6:42 PM Eric Springer : email: [ericwspringer@gmail.com](mailto:ericwspringer@gmail.com)  
6:42 PM Eric Springer : Address 620 STEWART ST, seattle, washington, 98101  
6:42 PM Mahesh (CSA) : Thanks for the confirmation.

Let me just stop right there, so I can point out that address *isn't mine*. It's just a fake address of a hotel that was in the same zip code where I lived. I used it to register some domains, knowing that the whois information all too often becomes public. I used the same general area as I lived, so that my ip address would match up with it.

Let's continue:

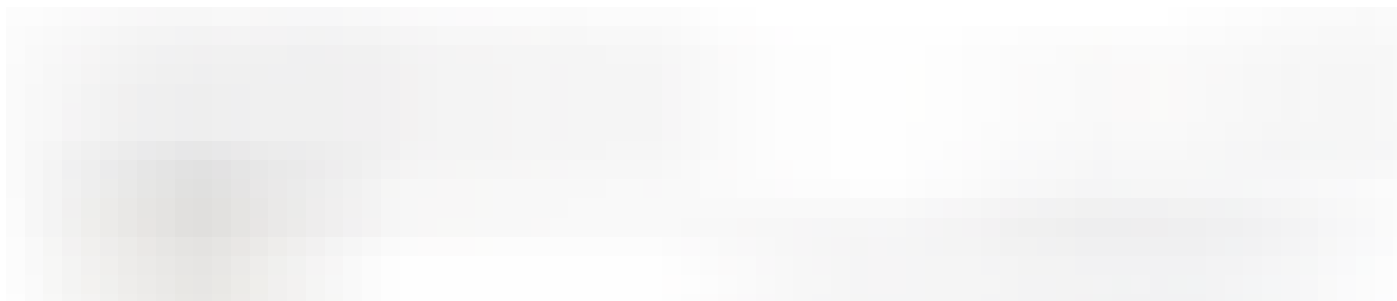


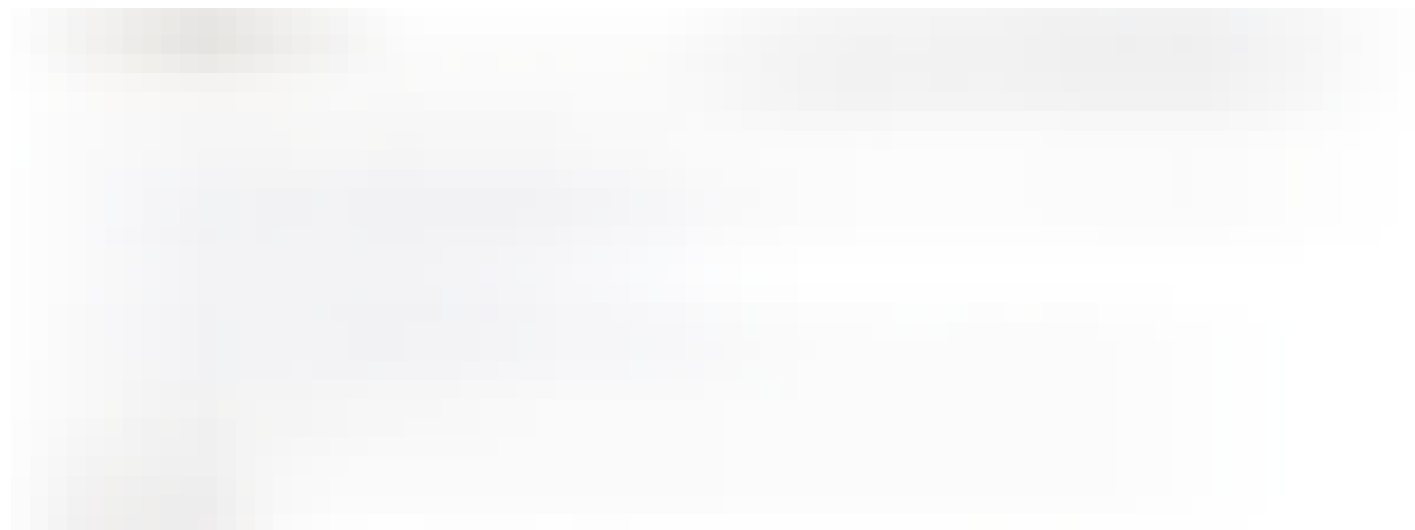
"That's all I needed".

Wow. Just wow. The attacker gave Amazon my fake details from a whois query, and got my real address and phone number in exchange. Now they had enough to bounce around a few services, even convincing my bank to issue them a new copy of my Credit Card.


Trying very hard to not take out my frustrations on an unrelated support rep, I contacted both Amazon Retail and AWS expressing my disappointment and asking them to put a note on my account that it is at extremely high risk of being social engineering, and I will always be capable of logging in. Amazon Retail said they would put a note, and have a specialist contact me (who never did) while AWS was dismissive of even a risk existing.

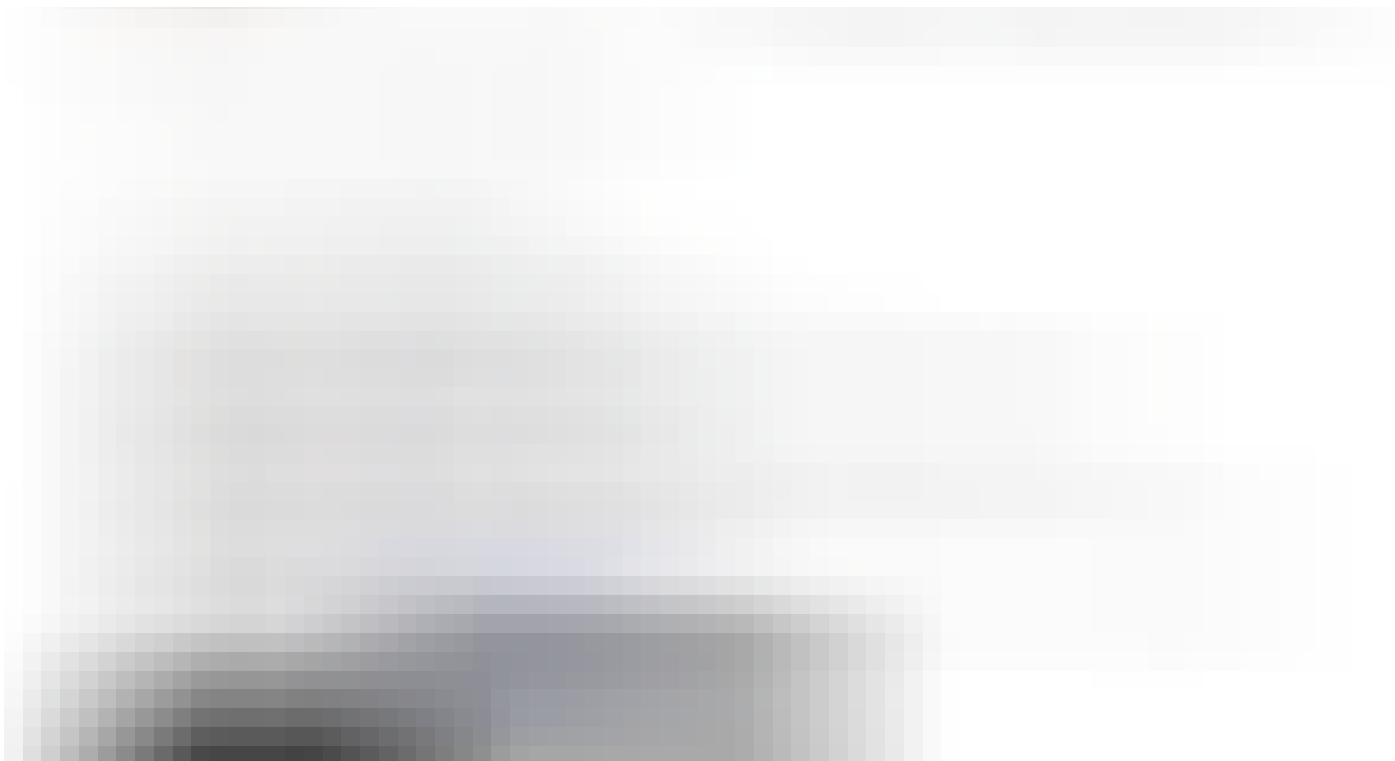
Fast forward a couple of months, I made the big mistake of thinking the risk was gone, giving Amazon my fresh credit card and now new address details. I receive another email. I feel a pit of my stomach.



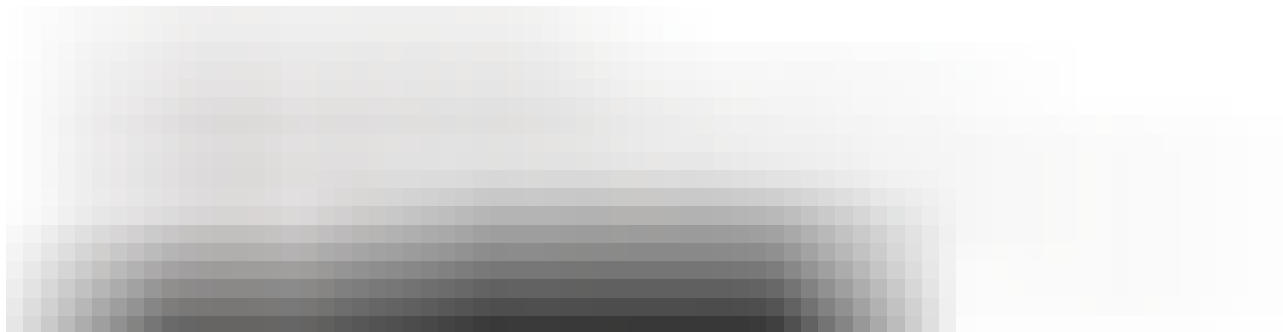


So once again, I contact Amazon support to see what happened. This time I had the pleasure of dealing with a support agent who seemed 100% incapable of realizing that someone was impersonating me. I had trouble keeping my composure when he told me I should change my password to prevent people impersonating me. Eventually I had to basically tell him that it was “me” that contacted support and I wanted “my” transcript, which he provided.



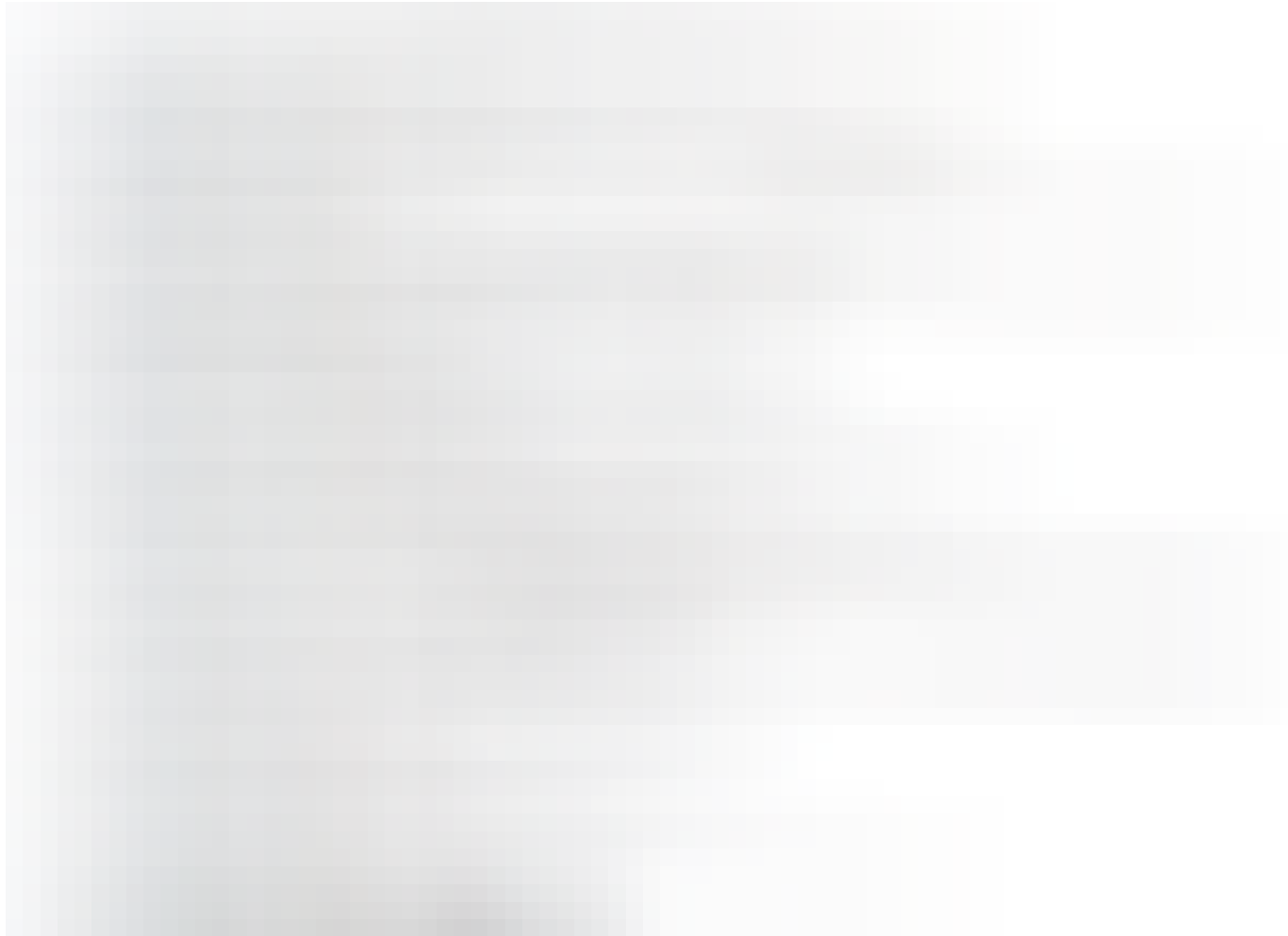


Using the address they got the last time from Amazon..



Again?! For fucks sake.

And then goes on to unsuccessfully try get the last digits of my credit card:



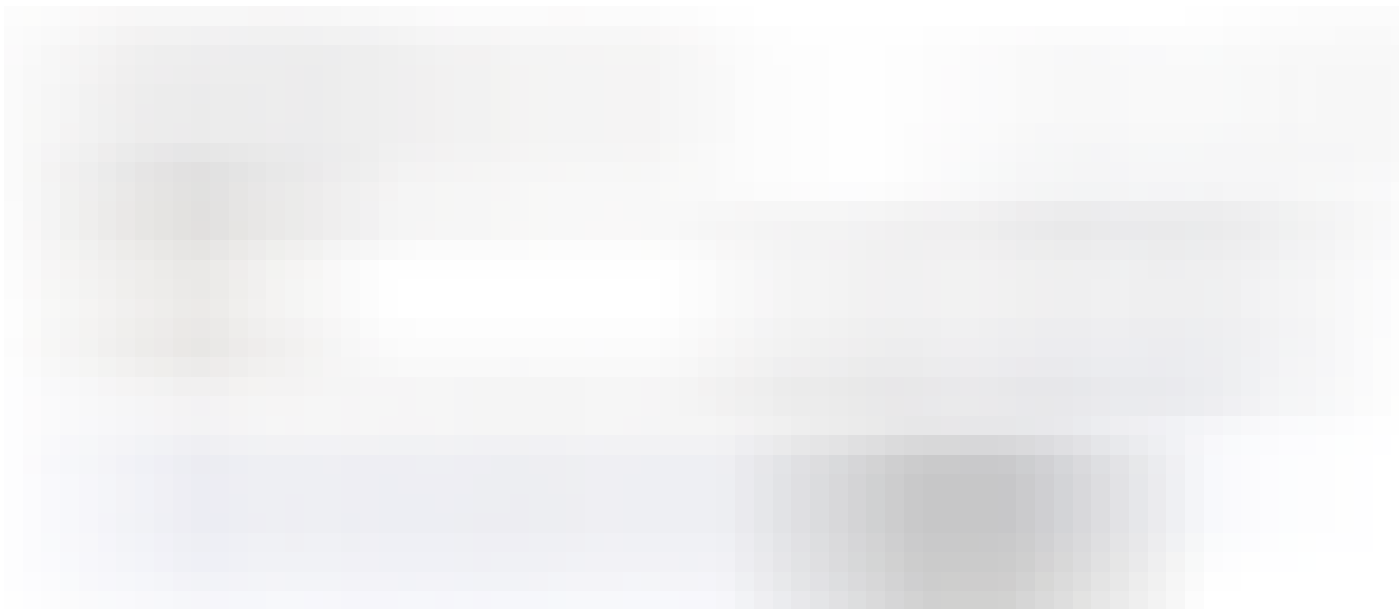
Yeah, that totally looks legit.



Guess I should count my blessings they didn't give the last digits of my credit card. I again contact Amazon to reiterate how important it is that they keep my account secure, and not give out my details to anyone with a name and address. They promise they're putting a note on my account, and it'll never happen again. And I will be contacted by a specialist (never happened, again)

This time I decide I can no longer trust Amazon with my address, and delete it from my account.

Fast forward another day:



This time, I can't get a transcript of the conversation. They contacted Amazon by phone, and they don't have a recording to give me. I'm going to have to assume they got the last digits of my credit card, like they seem to be after.

At this point, Amazon has completely betrayed my trust three times. I have done absolutely everything in my power to secure my account, but it's hopeless. I am in the process of closing my Amazon account, and migrating as much to Google services which seem significantly more robust at stopping these attacks.

After being the victim of these attacks for months, I'd like to make some recommendations for services:

- NEVER DO CUSTOMER SUPPORT UNLESS THE USER CAN LOG IN TO THEIR ACCOUNT. The only exception to this, would be if the user forgot the password, and there should be a very strict policy. The problem is, 9999 times out of 10000 support requests are legitimate, agents get trained to assume they're legitimate. But in the 1 case they're not, you can completely fuck someone over.

- Show support agents the ip address of the person connecting. Is it a usual one? Is it a VPN/tor one? etc. Give them a warning to be suspicious.
- Email services should allow me to easily create lots of aliases. Right now the best defense against social engineering seems to be my fastmail account which allows me to create 1 email address alias per service. This makes it incredibly difficult for an attacker when they can't even figure out your email.
- Please make whois protection default. Mine leaked because a stupid domain I didn't care about had its namecheap whois protection expire

For users, be extremely careful with the information you share. Even big companies like Amazon can't keep it safe, they're far from the worst.

Security

Privacy

Amazon

7K claps



140



Eric

Follow



Also tagged Privacy



## Why 'Anonymized Data' Isn't So Anonymous



Tyler Elliot Bettilyon

Apr 24 · 10 min read



196



Related reads



## In Chinese Spy Ops, Something Old, Something New

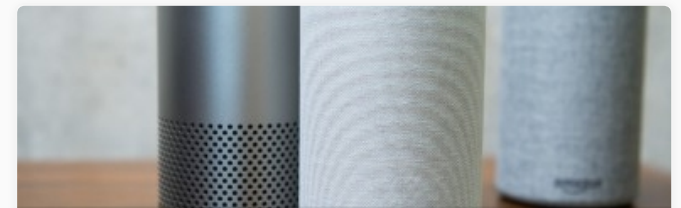


Foreign Policy

Nov 5, 2018 · 4 min read



83



Also tagged Privacy



## Amazon's Alexa Reviewers Can Access Customers' Home Addresses



Bloomberg

Apr 24 · 4 min read



1



### Responses



Write a response...

Conversation between :( and Eric.



:(

Jan 25, 2016

Thank you for sharing this... but I couldn't just accept this so I went ahead and did it to my own account. Unfortunately, you are right and I was able to get my own address with a fake hotel address as well... If interested see the following links for screenshots of the chat: <http://imgur.com/5JB08eH> and <http://imgur.com/6lruQu4>

300

6 responses 



Eric

Jan 25, 2016

The sad part of it all, is how some of the support reps don't seem to even to understand the idea of social engineering. The first time I contacted Amazon the agent was pretty cool, but the second time I got someone who calling clueless would be a compliment. I literally had to trick him into thinking I was the attacker, to see the transcripts.

37

1 response 

Applause from Eric (author)



Jessamyn West

Jan 25, 2016 · 1 min read

Really interesting. I used this same exploit to get access to my dad's accounts after he died and I had to change or close his accounts. It was so much easier

doing this as “him” via IM or phone calls compared to having to fax death certificates and executorship documents to cable and phone companies. I could not agree more that this is the weak link...

[Read more...](#)

137

1 response 

Applause from Eric (author)



**Chris Cardinal**

Jan 25, 2016 · 1 min read

I wrote up a similar wild gaping hole in Amazon’s customer support social engineering THREE YEARS AGO. And lo, it is still not fixed. With the “account trifecta” of a user’s name, billing address, and email address, you can get a customer support rep to give you all sorts of personal information, including order numbers, the contents of those orders...

[Read more...](#)

76



Applause from Eric (author)



**Dave Rutledge**

Jan 25, 2016 · 1 min read

I had a similar situation where the caller was allowed to try 3 or 4 addresses they found online, and the Amazon representative confirmed the correct one for them. Like with you, Amazon seemed to only be considering that people were trying to get access to the account, and they were unable to understand the potential problem of giving out personal...

Read more...

27



Applause from Eric (author)



Scott Hanselman

Jan 25, 2016

This exact chat scenario happened to me over two years ago. Not comforting that they haven't closed this hole.

<http://www.hanselman.com/blog/ChasingAnActiveSocialEngineeringFraudAtAmazonKindle.aspx>

62



---

Conversation with Eric.

Gary Larson





Jan 25, 2016 · 1 min read

Great article. I think I'm confused about something though. The attacker got your real address from Amazon because they told him where the last order was shipped to. Later in the post, you said you deleted your address from being saved in your account. How does this help? Even if your address wasn't stored in your account when the original attacks...

[Read more...](#)

7

1 response 



Eric

Jan 25, 2016

The reason I removed it from the system, was so when the attacker contacted Amazon they would have trouble authenticating as me (since the account has no addresses on file).

But yeah, didn't help.

10



---

Conversation with [Eric](#).

[Zach Queal](#)





Jan 24, 2016 · 1 min read

This is a serious case of what I've come to suspect in the past few months as well. About 2 months ago I received a fairly sophisticated phishing email designed to steal my Amazon login details. I noticed it right away, but decided to use Incognito Mode to access the URL to snoop around a bit. I didn't find anything revealing—but I decided to...

[Read more...](#)

93

1 response



Eric

Jan 24, 2016

That was my experience with AWS support too. I can't believe there isn't a "high-risk" setting, where you can opt-out of certain features (like support resetting your email).

58

1 response

---

Conversation between :( and Eric.



:(

Thank you for sharing this... but I couldn't just accept this so I went ahead and did it to my ow



Eric

Jan 25, 2016

Great screen captures!

7



[Show all responses](#)