

1000 New Stores Rocks Investors!

China Shoe Holdings Inc. (CHSH)

\$0.58

CHSH is rocking investors with recent plans to open 1000 new retail outlets over the next two years. More news is expected Monday and we are expecting huge trading in expectation of it.

Read the news and get on CHSH first thing Monday!

Unfortunately none of the advertisers in their initial survey were using auto-tagging to fix this problem, which results in inflated click fraud estimates.

We benefit greatly from the feedback our advertisers provide us, as it helps us constantly improve our systems and customer service, and we would always like to get more.

We have also been working on plans to share detailed click information, similar to a phone bill as many in the industry have pointed out.

The challenge is ultimately how do you detect the hard-to-detect click fraud attempts, regardless of their methods.

But most importantly, the fact that they don't take into account the amount that Google already protects advertisers against means that they're not even trying to measure actual click fraud.

But this type of report would provide advertisers further transparency into which clicks occurred on their ads and more easily identify discrepancies between their systems and ours.

Frankly, this entire post feels like Google trying to make nice with Fair Isaac and Fair Isaac make nice by Google by pushing out the blame on the media.

Incidentally, Neil is also the author of the recently published "Foundations of Security: What Every Programmer Needs to Know", which is a great reference as well as introduction to security methods.

We utilize a number of different automated techniques and algorithms, as well as a proactive manual analysis, to do this, analyzing hundreds of different factors.

Similarly, botnets can also be poorly designed, and their clicks easily detected and filtered.

But in practice this is not the case.

To begin, where do third-party click fraud numbers come from?

Focusing on the incorrect methodologies of the click fraud firms just deflects attention from the real issues.

I can appreciate how advertisers feel wronged by the fact that it's only in response to challenges that certain facts come to light, rather than as a part of general discourse.

A reload of the advertiser's landing does not contact Google again.

A reload of the advertiser's landing does not contact Google again.

We further qualified that there might be issues in terms of what's considered billed.

To begin, where do third-party click fraud numbers come from?

com from non-US countries will not result in the user opting into US results and ads.

Job Description: Civil and coastal engineering involving major US Navigation projects.

We obviously monitor for bot activity and have lists of known bots which we maintain.

Equal Opportunity Employer Go back to listings

Access Error Headline functionality has been disabled from your intranet.

Frankly, this entire post feels like Google trying to make nice with Fair Isaac and Fair Isaac make nice by Google by pushing out the blame on the media.

Botnets have of course been around for many years, and have been used most commonly for activities like denial of service attacks.

And that is exactly what our click quality team focuses on, and why it's important to stay ahead of fraudsters in technological sophistication.

Does Google not want the world to see the "crazy aunt in the basement spinning straw into gold" perhaps?

Perhaps the click audits are not providing sufficient consideration the tendency of consumer research.

They can tap into the knowledge of such people to find out anything they need to know about how the web works, etc.

, I imagine before long, they will.

Focusing on the incorrect methodologies of the click fraud firms just deflects attention from the real issues.

Or, is Google afraid to split this traffic onto a separate network?

Fair Isaac indicated that they needed a lot more data before they could conduct

a meaningful study.

But in practice this is not the case.

fr, we will show them ads geotargeted to France even if their computer is located elsewhere.

If you are the system administrator, please click here.

Geotargeting is based on IP address and other signals and works very well, but is not perfect.

Malware detection rates may need to be improved.

There are many different ways that click fraud is attempted, and the use of botnets generally represents one of the more sophisticated methods.

Contact Info: We offer a competitive salary and outstanding benefits package and a professional environment that supports development and recognizes achievement.

Both articles stresses this covered a handful of advertisers and couldn't be applicable to the industry as a whole.

Users can run anti-virus software to help prevent their computer from participating in a botnet.

Your arguments are not based on a clear presentation of evidence, but rather on a your summation of the data combined with your interpretation.

I agree with this, and we are currently working on ways to provide advertisers with more transparency into where their ads are placed.

By that point, there was also an AP article out.

" Analyzing botnets is an important activity in both our Click Quality and Security Teams.

Incidentally, Neil is also the author of the recently published "Foundations of Security: What Every Programmer Needs to Know", which is a great reference as well as introduction to security methods.

All contents available under a Creative Commons License.

We already qualified things perfectly fine.

Opinions on this web site are the author's own.

Many thanks to the advertisers who provided their suggestions, as well as to all of the other groups that send us ideas regularly.

They can tap into the knowledge of such people to find out anything they need to know about how the web works, etc.

They can tap into the knowledge of such people to find out anything they need to know about how the web works, etc.

Must be proficient in MS Word, Excel, Project and PowerPoint.

You're telling the world that people are misinterpreting user behavior when people click on the BACK button in their browsers.

We are in favor of submitting our systems to an audit by a trusted third party, and are working with the other members of the IAB Click Measurement Working Group to set this up.

Perhaps it hasn't yet been fully or correctly utilized, so the significant corrective drop in their numbers is yet to come.

Daily News Digest - One page daily news snapshot.

It seems to me that this type of discussion needed to be had long ago.

If it clicks too many times, it could be click fraud.

One reason we're publishing this paper is to continue to share more information on the types of analysis we do to protect our advertisers against click fraud.

Thanks again for your feedback, and I hope that helps.

We did an initial short write-up saying there was this new study out, there was limited data about it, and that it was far off the mark from what Google has reported.

This allows them to properly count clicks and avoid the problem of fictitious clicks we have discussed before.

This allows them to properly count clicks and avoid the problem of fictitious clicks we have discussed before.

But most importantly, the fact that they don't take into account the amount that Google already protects advertisers against means that they're not even trying to measure actual click fraud.

Botnets have of course been around for many years, and have been used most commonly for activities like denial of service attacks.

About an hour or two after our initial, qualified article, I took a deeper look at the IW article.

Read the lead, and it's pretty clear it was.

Unfortunately, that was a very technical report, which was difficult for many readers to parse.

Desired Experience: Strong communication, technical writing skills, and project management experience.

The Click Quality team helps diagnose these cases every day, but you as an advertiser can diagnose them too.

Thanks again for your feedback, and I hope that helps.

com from non-US countries will not result in the user opting into US results and ads.

A around the time the attack was publicly reported.

To begin, where do third-party click fraud numbers come from?

Fair Isaac put out a press release yesterday which has gotten coverage in a number of media outlets.

Incidentally, Neil is also the author of the recently published "Foundations of Security: What Every Programmer Needs to Know", which is a great reference as well as introduction to security methods.

Update: Search Engine Watch has additional details on this at "Fair Isaac Click Fraud Report Spreads False Alarm".

And that is exactly what our click quality team focuses on, and why it's important to stay ahead of fraudsters in technological sophistication.

We saw InformationWeek come out with the story first.

If it clicks too many times, it could be click fraud.

Unfortunately, these flawed estimates attract a great deal of publicity and must be debunked quickly before they mislead advertisers, users, and the industry as a whole.

The biggest difference is the fact that it requires unsupervised analysis, something they told us they are aware of.

Update: Search Engine Watch has additional details on this at "Fair Isaac Click Fraud Report Spreads False Alarm".

Unfortunately none of the advertisers in their initial survey were using auto-tagging to fix this problem, which results in inflated click fraud estimates.

On a related issue, it strikes me that it's taken over a decade now for open discussion of these matters, limited as it is.

IP frequency is the number of times an IP address clicks within a certain time window.

You wonder why someone might think this is put out as an industry standard?

, which make this much more than just a generic task for existing fraud tools from other industries.

There are several free offerings available to users in the market.

Once a user visits that page, they often browse through the site, navigating through sub pages, and then return to the original landing page by hitting the back button.

Read the lead, and it's pretty clear it was.

Send feedback on this article [Digg it](#) or [bookmark with](#).

I agree that advertisers should not be charged for double clicks.

I'll try to provide a simpler explanation [here](#).

There are several free offerings available to users in the market.

In other words, is it possible that through study of the Internet architecture, fraudsters can not only discern these means, but devise means of their own of thwarting them?

I'm planning on writing more about that here too.

If we made that information public it would open our advertisers up to enormous risk.

Does Google not want the world to see the "crazy aunt in the basement spinning straw into gold" perhaps?

People are not inclined to trust that kind of response regardless of how sensitive the data being evaluated truly is.

A case at our AdWords Blog post, and you can access Neil's paper, which he co-wrote with Mike Stoppelman and other team members, here.

We also found that in other instances, clicks classified as "click fraud" by third-party firms produced sales at the same rate as the "good" clicks.

These are features which provide targeting controls to advertisers and are more similar to geotargeting than anything related to invalid click detection.

A case at our AdWords Blog post, and you can access Neil's paper, which he co-wrote with Mike Stoppelman and other team members, here.

Sure, later down you get this: "These are early results based upon a limited view of the market," said Milana.

You call this archeology?

In the rare event you find that your campaign may have been affected by undetected click fraud, our Click Quality team definitely wants to hear from you.

Like I said, we didn't need it.

Access Error Headline functionality has been disabled from your intranet.

If it clicks too many times, it could be click fraud.

To begin, where do third-party click fraud numbers come from?

Users can run anti-virus software to help prevent their computer from participating in a botnet.

Around the time the attack was publicly reported.

So is there a solution to this?

So we're not looking to identify a botnet or a click farm so much as we're trying to identify potentially malicious or fraudulent clicks.

On a related issue, it strikes me that it's taken over a decade now for open discussion of these matters, limited as it is.

Additionally, GBA provides services in hydrographic surveying, coastal engineering and channel design.

So we're not looking to identify a botnet or a click farm so much as we're trying to identify potentially malicious or fraudulent clicks.

Many of the domains and hosts involved in conducting the attack described in this paper were compromised.

They can tap into the knowledge of such people to find out anything they need to know about how the web works, etc.

com, the Engineering Job Source

Both articles stresses this covered a handful of advertisers and couldn't be applicable to the industry as a whole.

I'll be answering the questions you and others have asked recently in my following posts.

Like I said, we didn't need it.

It would contain information such as the IP addresses, time, and cost associated with individual clicks.

Because of our investment in click fraud protection systems, we are able to manage this issue very well and prevent it from having an impact on the vast majority of AdWords advertisers.

We benefit greatly from the feedback our advertisers provide us, as it helps us constantly improve our systems and customer service, and we would always like to get more.

Until then, the short answer is that our click fraud protection systems analyze data in a way that is generally independent of the source or method used for the attack.

I spoke with Joe Milana, chief scientist at Fair Isaac, today to find out what the real story was.

A reload of the advertiser's landing does not contact Google again.

In fact, we are hosting our first advertiser forum dedicated exclusively to invalid clicks at Google headquarters this coming week.

I thought folks might be interested in where Google stands on some of their requests.

We obviously monitor for bot activity and have lists of known bots which we mai

ntain.

But that is actually not even the most common problem with their analyses.

It's that you have not substantiated your points by showing conclusively that these are the primary causes of misinterpretation of data.

Or, is Google afraid to split this traffic onto a separate network?

Both articles stresses this covered a handful of advertisers and couldn't be applicable to the industry as a whole.

Users can run anti-virus software to help prevent their computer from participating in a botnet.

Advertisers can already obtain referrer URLs from their own web logs, of course .

But heck, we added the Google comments anyway.

By utilizing thousands of hijacked IPs, a fraudster hopes that their attack will be difficult to catch.

Until then, the short answer is that our click fraud protection systems analyze data in a way that is generally independent of the source or method used for the attack.

We utilize a number of different automated techniques and algorithms, as well as a proactive manual analysis, to do this, analyzing hundreds of different factors.

Click fraud detection does not require unsupervised analysis, and supervised classifiers are routinely used when conversion or other similar post-click data is available.

It would contain information such as the IP addresses, time, and cost associated with individual clicks.

Perhaps the click audits are not providing sufficient consideration the tendency of consumer research.

The Click Quality team helps diagnose these cases every day, but you as an advertiser can diagnose them too.

Like I said, we didn't need it.

Fair Isaac put out a press release yesterday which has gotten coverage in a number of media outlets.

com, the Engineering Job Source

Focusing on the incorrect methodologies of the click fraud firms just deflects attention from the real issues.

In other words, is it possible that through study of the Internet architecture, fraudsters can not only discern these means, but devise means of their own of thwarting them?

Google can count ad clicks reliably as a click on a Google ad will cause the web browser to contact Google and then we redirect it to the advertiser's landing page.

Perhaps the click audits are not providing sufficient consideration the tendency of consumer research.

We benefit greatly from the feedback our advertisers provide us, as it helps us constantly improve our systems and customer service, and we would always like to get more.

The net result was that advertisers were consistently being given false data from reports they trusted, which would actually hurt their advertising campaigns if they acted on them.

The audit will likely be administered through the Media Ratings Council, the organization which audits Nielsen and Arbitron.

There are several free offerings available to users in the market.

Once a user visits that page, they often browse through the site, navigating through sub pages, and then return to the original landing page by hitting the back button.