World Cup fans are the latest to be targeted by cyber criminals

July 11 2014, by Nik Thompson

We're most at risk from cyber scams when distracted by events such as the World Cup. Credit: Flickr/Nelson Oliveira, CC BY-NC

As rival football teams have been battling it out in this year's World Cup, cyber criminals have had their eye on a different goal – to cash in on this global distraction at any opportunity.

Among the legitimate marketing campaigns, these cyber criminals have been trying to exploit the public's enthusiasm for the most watched and most profitable sporting event in the world, attracting 400 million views per match.

In the run up to the 2014 FIFA World Cup, as many as 50 fraudulent websites were shut down daily in Brazil alone.

Links to these fraudulent websites are spread by massive spam campaigns sending billions of spam messages daily to dupe unwitting fans into opening links which lead to fake ticket websites, cash giveaways and attempts to steal personal data.

Some of these are so convincing that even Brazil's own Ministry of External Relations has been caught out. Hackers even managed to take down the official websites of the Sao Paulo Military Police and the official World Cup 2014 Brazil.

Are you part of the spam scam?

It takes just one momentary lapse in judgement to become a victim of some online scam. Worse still, your computer could be silently taken over, turning you into an unwitting spammer.

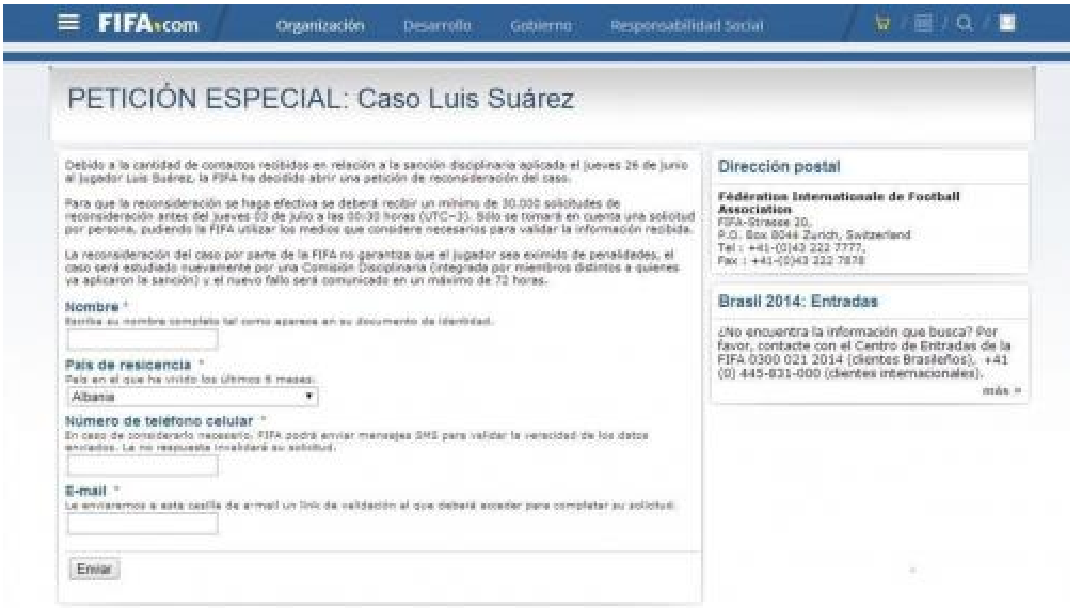
Latest figures from the security firm Kaspersky show 69.8% of the world's total email traffic is spam. The public have grown so accustomed to ignoring the problem that few actually understand where spam originates, or realise that they themselves might be spammers.

But how do underground criminals successfully operate a computer network large enough to send out 200 billion email messages per day ?Well, this is where you come in.

A botnet (short for robot network) is a collection of thousands of malware (malicious software) infected computers that are under the control of criminals.

Botnets are assigned tasks by the botnet operator, including sending spam, or distributing even more malware to increase the size of the botnet. They are also used for spying, stealing banking details, holding your computer to ransom and more.

A large botnet might contain tens of millions of infected computers, whose owners are entirely oblivious to the situation. Infection spreads via spam campaigns or compromised websites and visitors may become part of the botnet without ever knowing.



PETICIÓN ESPECIAL: Caso Luis Suárez

Debido a la cantidad de contactos recibidos en relación a la sanción disciplinaria aplicada el jueves 26 de junio al jugador Luis Suárez, la FIFA ha decidido abrir una petición de reconsideración del caso.

Para que la reconsideración se haga efectiva se deberá recibir un mínimo de 30.000 solicitudes de reconsideración antes del jueves 03 de julio a las 00:30 horas (UTC−3). Sólo se tomará en cuenta una solicitud por persona, pudiendo la FIFA utilizar los medios que considere necesarios para validar la información recibida.

La reconsideración del caso por parte de la FIFA no garantiza que el jugador sea eximido de penalidades, el caso será estudiado nuevamente por una Comisión Disciplinaria (integrada por miembros distintos a quienes ya aplicaron la sanción) y el nuevo fallo será comunicado en un máximo de 72 horas.

Nombre *
Escriba su nombre completo tal como aparece en su documento de identidad.

País de resicencia *
País en el que ha vivido los últimos 6 meses.
Albania

Número de teléfono celular *
En caso de considerarlo necesario, FIFA podrá enviar mensajes SMS para validar la veracidad de los datos enviados. La no respuesta invalidará su solicitud.

E-mail *
Le enviaremos a esta casilla de e-mail un link de validación al que deberá acceder para completar su solicitud.

Enviar

Dirección postal

Fédération Internationale de Football Association
FIFA-Strasse 20,
P.O. Box 8044 Zurich, Switzerland
Tel : +41-(0)43 222 7777,
Fax : +41-(0)43 222 7878

Brasil 2014: Entradas

¿No encuentra la información que busca? Por favor, contacte con el Centro de Entradas de la FIFA 0300 021 2014 (clientes Brasileños), +41 (0) 445-831-000 (clientes internacionales).

más »

An online petition made to look like an official FIFA website but revealed as a phishing scam.

World Cup scams

Scammers are always on the lookout for new tactics to lure in their victims. For instance, right after the Uruguay vs Italy match an online petition appeared for fans to register their support against the disqualification of Uruguayan striker Luis Suarez.

Fans flocked to the website, sharing it with friends and across social media, although the "petition" was in fact yet another scam to harvest personal information.

Upfront payment or money transfer scams are another favourite used by scammers. Often known as "Nigerian Scams", these advise potential victims by email that they are entitled to a large sum of money, but that the victim may need to send personal details or a cash advance to cover "administration costs".

One such scam is doing the rounds informing recipients that they have won UK £3 million from the FIFA World Cup organising committee.

The most striking thing about these emails is that they are usually poorly worded, full of grammatical errors and often look extremely suspicious.A question that springs to mind is why don't the scammers try to be a bit more convincing?

Research from Microsoft on Nigerian scams provides an answer – the scams are deliberately made as obvious as possible so that they entice only the most gullible people to reply.

An email with tales of fabulous amounts of money and West African corruption will strike all but the most gullible as bizarre. It will be recognized and ignored by anyone who has been using the Internet long enough to have seen it several times […] Those who remain are the scammers ideal targets.

Spam botnets make light work of contacting millions of potential victims, but the crooks don't want to waste their time talking to people who are likely to see through the scam.

In the words of the the report's author, Micosoft researcher Cormac Herley: "Anybody who doesn't fall off their chair laughing is exactly who they want to talk to."

It's not all bad

Computer security begins with an appreciation of the risks present in our online environment. Unlike business users who have advice on hand and the benefit of IT support, home users often simply fend for themselves.

Fortunately, resources such as the Australian Government's ScamWatch and Stay Smart Online provide security advice for home users with many other excellent resources just a web search away.

If you suspect that your computer might already have been infected by malware, then free tools from vendors such as Sophos or Kaspersky can find these threats.

A valuable tip is to not rely on one security software to detect everything. Certain tools are better at finding particular threats, so scanning with multiple tools can be beneficial.

The World Cup will soon be over but the scams will continue as the cyber criminals simply find another event or campaign with which to trap the gullible.

So it's wise to heed words of warning from the networking giant Cisco Systems in its 2014 Annual Security Report:

[…] there should be an assumption by all users, perhaps, that nothing in the cyber world can or should be trusted.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: World Cup fans are the latest to be targeted by cyber criminals (2014, July 11) retrieved 20 March 2024 from https://phys.org/news/2014-07-world-cup-fans-latest-cyber.html