Bad Ads Spotlight: Ads Promoting Free Software Downloads

February 2015

TrustInAds.org
Keeping people safe from bad online ads

OVERVIEW

Today's consumer has the ability to tap into a diverse set of software applications available on the Internet to install at the click of a button. Developers of these applications will often promote their software via online advertising to make their apps more accessible to potential users. In addition, countless "free" options for any particular type of software also exist. For the consumer, it can sometimes be difficult to understand the features and expected behavior of an app, even after it has been downloaded and installed on a computer or mobile phone.

Be it for computer screensavers, operating system cleaners, or antivirus software, "free" is certainly an enticing offer, and many types of downloadable software do not pose a problem for consumers. Unfortunately, there are some bad actors out there that have developed apps can be tremendously harmful.

Some scammers promote software that can introduce a variety of consumer harms - all without the consent or knowledge of the user. For example, they can infiltrate a user's computer to introduce malware and other security vulnerabilities. The software can also rewire the browser's default settings, act like unwanted adware that injects inappropriate or scammy ads on webpages, or install malicious code that can capture sensitive user information or even hijack the computer.

The National Consumers League (NCL) recently highlighted this issue as well (http://www.nclnet.org/scammy_software), noting the dangers of some of these kinds of tempting offers.

Because some of these scammers are attempting to use advertising to reach consumers, TrustInAds.org companies are on the look out for these advertisers. For example, Google has been regularly identifying and disabling advertising for programs that are misleading, don't behave in ways that are clear to users, or otherwise make undisclosed system changes.

Our member companies work tirelessly to identify and reject these types of ads, but bad actors continue to look for ways to bypass the automated filtering and manual review processes the company has in place.

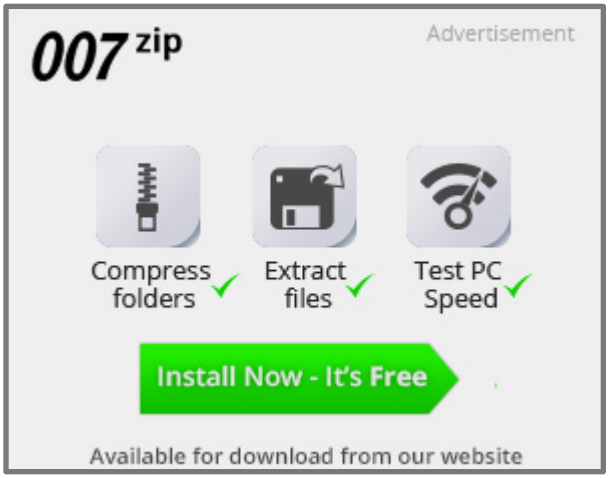
We continue to monitor their platforms for these types ads, and we will provide updates as any new information is gathered.

EXAMPLES OF BAD ADS AND SOFTWARE IMPACT

Below are examples (Figs. 1, 2) of ads that, after review, were removed from Google's platform.

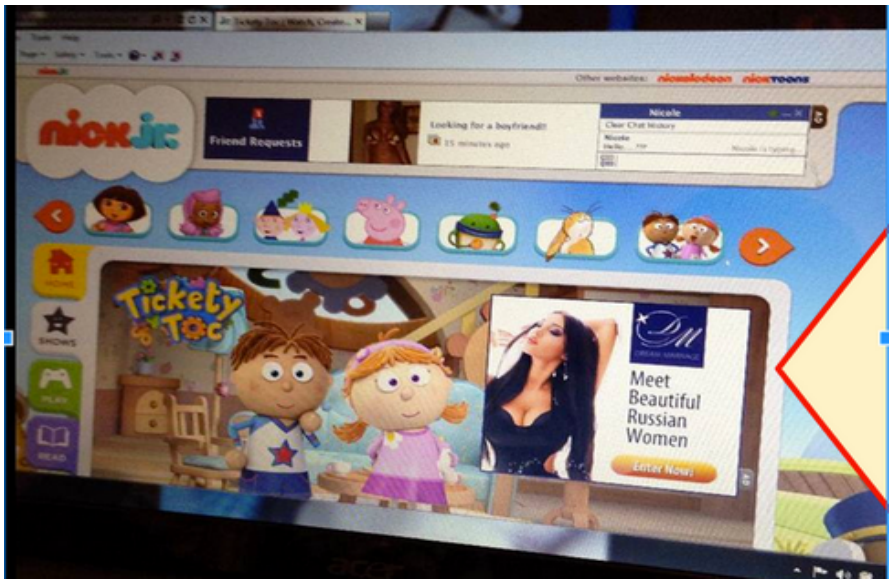
Fig. 1

Fig. 2



Additionally, below is a screenshot provided by a user that shows how this type of software can impact consumers. Through a surreptitious change in browser settings, a downloadable application injected these inappropriate ads on top of a child directed website.

Fig. 3



ACTIONS TAKEN BY GOOGLE

To address this issue, Google uses information from user complaints to identify problem ads and advertiser accounts and cross-references them against others with similar attributes. From this information, the company creates automatable signals that are built into the enforcement algorithms. Also, through machine learning, the different systems can teach themselves to flag similar ads going forward.

Since this process began, Google has removed approximately 6,500 suspicious advertiser accounts linked to approximately 250,000 websites distributing malware and unwanted software.

TIPS TO CONSIDER WHEN ONLINE

TrustInAds.org urges consumers to consider the following suggestions when online.

- **Understand the software**. You should always strive to understand any software that you download to make sure that it does not contain malware or unknown add-ons. Read the disclosures from the software's site and don't agree to "add-ons" or "additional offers" that you do not understand.

- **Keep your browser up-to-date**. When your browser notifies you that it's time for an update, do so as quickly as possible. These updates often include important security fixes to patch previously identified vulnerabilities.

- **If you see a suspicious advertisement on any of our platforms, REPORT IT**! As we highlighted in our previous reports, one of the best ways we can defend users from harmful scams and bad ads is through user feedback. The TrustInAds.org member companies have simple ways to alert them of potential scams and bad ads. Visit http://TrustInAds.org/report to learn how.

  Users should also file a complaint with FTC by visiting http://ftc.gov/complaint.

  And if you believe your personal financial information has been compromised, we encourage you to visit the FTC's consumer information section of its website regarding identity theft (http://www.consumer.ftc.gov/features/feature-0014-identity-theft).

ABOUT TRUSTINADS.ORG

TrustInAds.org comprises a group of Internet industry leaders that have come together to work toward a common goal: Protect people from malicious online advertisements and deceptive practices. With this effort, TrustInAds.org and its member companies are: Bringing awareness to consumers about online ad-related scams and deceptive activities; collaborating to identify trends in deceptive ads and sharing best practices; and sharing our knowledge with policy makers and consumer advocates around the country. To learn more, visit http://trustinads.org.

Follow us on Twitter, Facebook and Google+.