Is personal information on the Internet still protected?

Let's take a look at the major threats to personal information on social networks as well as in the advertising content on the Internet.

***TipsMake.com* - Let's take a look at the main threats to personal information on social networks as well as in the advertising content on the Internet .**

Barry Hoggard in New York outlines a limit to the protection of personal information online. Hoggard has deleted his Facebook account that has been used for the past 4 years and said goodbye to 1251 friends on this social network to protest against what he calls policies that are abusing privacy. on social networks. Speaking of changes in Facebook's recent privacy protection policy, the computer programmer said: " *I was tired of having to update security settings on Facebook to protect myself. "I don't have too much expectation about securing personal information on the Internet, but Facebook has gone too far."*

For Facebook or with advertisers can reveal personal information of users as well as those who can find the address of the city you live in, new ways to use technology also As using the Internet is making matters of personal information protection more controversial than ever.

Jeffrey Chester, director of Center for Digital Democracy, a nonprofit organization that promotes the privacy of online personal information and freedom of speech, said: 'Now, the Personal information is no longer the same as a year ago. We were worried about ads going to spread viruses into personal computers. ' In today's trends, keeping control of personal information becomes more difficult than a year earlier. Here are some threats to the

privacy of information online:

Social networks

Are social networks an omen of the privacy of personal information online? Many people who have just left Facebook say that is true. And there are also many users of Facebook's 450 million existing customers who consider the company an example of security for other social networks.

Facebook appeals to users in that it allows people to chat and share images. But gradually, users find their personal information shared to many other people, especially advertisers. In May, Facebook changed a number of personal information protection policies, which used to reveal users' information to market activists.

One of those changes is related to Instant Personalization. This program allows selected objects on Facebook to access the user's personal data and content. When Instant Personalization is activated, users' Facebook information can be compromised when users visit other people's sites, including Microsoft's Docs.com, Pandora and Yelp. When the program was released in April, Facebook activated the program for all users. However, the company also had to review this policy due to concerns surrounding the protection of personal information. Now, users have the option to choose whether to install Instant Personalization or not.

Previously, Facebook's personal information protection policies were once considered backward. In 2007, the company launched Beacon, an advertising system that allows to track the specific behavior of Facebook users on 44 partner sites to record these behaviors on Facebook of friends who are friends. user's. However, many users have objected to this system due to concerns about personal information protection. Facebook CEO Mark Zuckerberg then quickly apologized to the user and turned Beacon into an optional feature on Facebook.

Marc Rotenberg, director of Electronic Privacy Information Center (EPIC), said: ' *Facebook is increasingly losing user protection of personal information* .' In early May, EPIC and 14 other customer groups filed a protest against Facebook to the Federal Trade Commission, accusing Facebook of revealing user personal information, which violated the original. Fair business rules.

Google Buzz (the social network of the Google search giant) also faces problems protecting users' personal information. Launched at the beginning of the year, Buzz revealed a list of users who often access email addresses.

According to Jeremy Miskin, a lawyer specializing in personal information protection issues, social networks have forced users to rethink the issue of protecting personal information in a world where public disclosure Personal information is one thing that is becoming popular. According to Mishkin, *'what's really important here is how Facebook ensures users can control their personal information'*.

Facebook declined to interview, but made the announcement: *'It is important that Facebook and other sites allow users to clearly control what information they want to share, when they want to share and share. With whom. We are listening to customer reactions and considering the best way to solve '.*

Data collection

Creating a personal information page will be easier if users use Facebook or Google Buzz. Market researchers will use information about users' preferences, such as the car manufacturer Volkswagen will use information to promote their new Jetta. And people wondered whether the information was used by credit institutions, medical service providers or business leaders.

Some firms, like California-based Rapleaf, said they are working with financial institutions to run email address data to collect customer information based on information shared on them. Social Network. Joel Jewitt, vice president of business development for Rapleaf, said the company has partnered with the company's marketing department, not a credit-accepting room, to target bank customers of financial services. .

Rapleaf is just one of many firms, from Acxiom to Unbound Technology, that uses social networks to get information. If a company wants to know information about users, they can use social networks.

For activists about protecting personal information, online advertisers are often very smart about issues related to their interests. Now, two strong emerging trends in advertising issues make it difficult for organizations to protect personal information that Madison Avenue has gone too far.

The first trend is that advertisers will combine online data and offline data to create digital records of Internet users. Companies like BlueKai, DataLogic and Nielson are partnering with online advertisers to help them reach Internet users with ads based on common behavior and population patterns. Advertisers have been careful to indicate that only verifiable and non-personal information is used and the user will never be identified by name but will be based on small population groups. . Display an advertisement banner to a certain group of people, such as the audience with information: a Capca mother has 3 children, 34 years old, an income of US $ 120,000, working 4 hours / week for a beauty center, it is perfectly acceptable.

An email address can create a link to personal information pages that aggregate online behaviors from sites like social networks. By exchanging this email address, advertisers can display banner ads according to spending habits and political views on Twitter.

See page 2

Real-time advertising technology

The second trend is technology that allows advertisers like Google and Yahoo to track users online and provide customized third-party advertisements at very fast speeds.

The way this technology works can be described as follows: When users access from page to page, advertisers can bid to have the right to display an ad. For example, if the user is looking to buy a Nikon digital SLR camera, users can see an advertisement of a Canon DSLR competitor on the next page they visit. If users buy a Canon, advertisers will be priced to have the right to show ads about the camera's lens.
Advertisers can track users from one page to another if they have the same advertiser and offer the same type of advertising. For example, Google Double Click provides ads to thousands of popular Web addresses. This real-time ad pricing program is called DoubleClick Ad Exchange.

The emergence of these two online advertising trends can create effective advertising strategies aimed at users' online income, interests and behaviors. However, security policy makers say that advertising has gone too far and advertisers are watching users unfairly and are making profits from user data themselves. .

Ed Mierzwinski of Public Interest Group said: *'Users will be surprised to find that companies can immediately combine the user's online information with previous data that users use is not known, let alone agree with this action '.*

Chester Jeffrey of Digital Democracy believes that this type of advertising is nurturing parasitic ads. Typical examples are vague treatments and high interest loans on HDTVs.

CDD, PIRG and World Privacy Forum have asked the Federal Trade Commission to consider advertising networks such as Google and Yahoo networks. These organizations are working to find transparency in advertisements and to find a way for customers to choose not to use personal information.

According to the Ponemon Institute, which researches personal information security, advertisers are sensitive to concerns about personal information protection. Ponemon said such worries motivated advertisers to use behavioral ads that were only 75% of what they wanted.

Transparency is a key factor for advertisers, according to Scott Meyer, president of Better Advertising. He said the advertising industry has stepped up efforts to avoid government regulations by developing self-defined programs. One of them is using transparent icons: Click on an icon on an ad and it will indicate whether the ad uses population and behavior data.

Better Advertising also offers a browser called Ghostery. This browser can warn users about the objects that are following you. Chrome, Firefox and Internet Explorer also support Add-ons but do not have program blocking, except Chrome.

Mobile devices

If it is not possible to manage a smartphone that installs GPS or manages geographic services, users can only blame themselves with the Big Brother service. Here are the reasons:

Mobile social networks like Foursquare, Gowalla and Loopt are designed to help friends know the shops, bars and shopping addresses of Facebook users. The iPhone and Android mobile applications use geographic location information. Facebook said that by the end of this summer, the company will announce features that make it easy to share geographic information like updating personal status on Facebook.

These services make the supporters of the protection of personal information on the web speak out and advise users to be careful about sharing information about themselves. In February, organizations protecting personal information asked lawmakers to limit which ads are allowed to retrieve user information. They argue that the guidelines for protecting personal information for services and advertising are obsolete.

For the point calculation service for members who show the accommodation is also worrying users. Peter Eckersley, technologist of the Electronic Frontier Foundation, said: *'Users should consider whether they want to disclose information about their place or location. For example: Do you go to church? Is there a political meeting? Is there a nightclub? Are you going to the beach on Tuesday? Can anyone need this information against you? '*

Mobile advertising goals

Some experts worry about advertisers eager to enter direct marketing on devices and mobile networks. Mobile social network Loopt said it is developing an advertising service aimed at repeating a store address for users. The company said advertisers wanted to influence customers' buying decisions.

Apps on smartphones such as the iPad are also worrying about privacy protection for activists. Chester of CDD said: *'With the help of GPS technology, every advertiser will know where you are and what you're doing on your phone.'* Mobile applications, even e-books, will know which stores are near you, near any restaurant or how far away you are from the clinic .

When will users feel safe?

What is the future of securing personal information? Will we all agree with Mark Zuckerberg, Facebook's CEO, who has a famous speech in 2009 *'the era of privacy protection has expired'?* Meyer of Better Advertising believes that the feeling that someone is watching will be dispelled when the development of technology allows users to better control their personal information as well as the transparency of services increased. Perhaps by then, we will have a sense of security.