How to survive the internet!

Mon, 24 Mar 2014 17:00:00, newstips66, [category: brotopia, post_tag: cargate, category: elon-musk, category: google-alphabet, post_tag: internet-privacy, post_tag: internet-tips, category: netflix, post_tag: the-cloud, category: web-spying, category: worldnews]

How to survive the internet!

(Give your friends the link to this page: http://wp.me/p4e1uX-26D)

(Check Kim Kommando for more updates)

WEB-PROTECTION

1. Never log in to anything.

Never sign in to anything. Only use Apps and sites that do not use a login and keep you anonymous. Do not let the internet know that you are using the internet or you will instantly be targeted. EVERY government network has already been broken into at least a dozen times. Every retail network has been broken into nearly a hundred times.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

2. Never send unencrypted email.

Always use GPG, or other encryption, and change your password weekly.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

3. Never backup or save files on "the cloud".

When you put files out on the web on other services you quadruple the ease with which your files can be broken into and stolen. It is like leaving all of your notebook computers on the curb every night.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

4. Don't buy any hardware unless it is open-source certified, globally, to be *"back-door free"*.

Many companies built spy door gates into their hardware but now all of the hackers have the keys to those doors. If you have un-certified servers, routers, wifi, etc. then the gates of hell are wide-open to any hacker these days.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

5. Never buy anything online with an account that has more than $200.00 in it.

Have one account only for buying things online and never connect it to any other account and never put more than $200.00 in it. Expect your accounts to be hacked and your money to be stolen.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

6. Always remember you are 3 CLICKS FROM DISASTER any time you are connected to a network.

These days, ANYBODY can take everything of yours off of ANY electronic device with just 3 clicks of most modern hacking software. BE CAREFUL!

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1 **7. Always use fake ID, Disinformation and a false name if you must log-in to a service like NETFLIX or other subscription service.**

You will be tracked, tagged and used **like this** if you don't.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1 **8. Never post your picture online or you will be processed with imaging comparison software by third parties.**

See this article about how **dating sites sell your image** but hundreds of others run image comparison software on every image on the internet and **abuse them for marketing too.**

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

9. Never keep ANY files on your computer!

Keep your Outlook .pst files, your photos, your documents, your movies and EVERYTHING you create, on an external encrypted hard drive. NEVER connect that hard drive to your computer unless your internet connection is physically unplugged and your wireless connection is removed or turned off in a way that you can check that it is turned off. If your mobile device is "always connected", ANY kid can take EVERYTHING off of it, with just two mouse-clicks, any time they want to. It IS OK to keep fake files on your computer to keep hackers on a wild-goose chase.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

10. Tape over any camera on any device you own.

ANY kid can secretly turn your camera on and watch you taking a shower, getting undressed, cheating on your partner, having sex or writing your secrets, with just two mouse-clicks, any time they want to.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

11. Don't use the CONTACTS and CALENDER in OUTLOOK, ICAL or on your device.

ANY kid can now download all of your contacts off of your phone and computer and watch them as well. A business competitor can download all of your calender appointments and bug your business meetings or get your business meetings cancelled. An ex lover and see who your new lover is and mess with that. Foreign countries can EASILY steal your technology

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

12. ALWAYS, ALWAYS pull the battery out of your device when you are not immediately using it

ANY kid can now download all of your contacts off of your phone and computer and watch them as well. A business competitor can download all of your calender appointments and bug your business meetings or get your business meetings cancelled. An ex lover and see who your new lover is and mess with that. Foreign countries can EASILY steal your technology. You device may appear to be turned off, you may have even seen it "turn off" but it is still on and pretending to be off.

Otherwise: *"Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"*

BNNERT1

FOR MORE DETAILS SEE THIS SERIES OF TIPS FROM A VARIETY OF SOURCES>>>(CLICK HERE)>

TD- LAT, GH-NYT, Steven Punter, Emilee Wiston

Inside the shadowy world of data brokers

CIO

From: www.cio.com

Inside the Shadowy World of Data Brokers

– Matt Kapko, CIO
Most consumers would not recognize the names of the large data brokers that constantly collect detailed information on their finances, health and other personal information. It's safe to say most people probably have no idea this is happening at all. Those who are aware should be shocked by the extent to which their online and offline behaviors are being sifted through for profit.

Call it panning for gold in the digital age.

The World Wide Web has always been a vehicle for advertising, but as the Internet permeates every facet of society from our apps to our appliances its role is expanding in kind. While surfing the Web or updating social apps on our smartphones, we blindly share valuable information about ourselves often without considering the ramifications - or, in some cases, even knowing we are sharing it.

[Related: FTC's 'Reclaim Your Name' Alone Won't Rein in Data Brokers, Experts Say]

Despite these growing privacy concerns, without advertising the Internet would deliver very few of the experiences many of us enjoy today. Companies need to be profitable to survive, and for most that path to revenue is advertising. While companies like Facebook and Google capture most of their data through consumer-facing products and services they offer for free, outside firms are collecting and organizing virtually all activity elsewhere.

'The Dark Underside of American Life'

As 2013 came to a close, Sen. Jay Rockefeller (D-W.Va.) issued a scathing report about the role and unchecked power of data brokers. Following a year-long investigation by the Senate commerce committee into the collection, use and sale of consumer data for marketing purposes, he called these companies and their practices "the dark underside of American life."

"Your smartphones are basically mini tracking devices that supply the kind of information that really talks about who you are on a day-to-day basis."

--Federal Trade Commissioner Julie Brill

"In 2012, the data broker industry generated $150 billion in revenue. That's twice the size of the entire intelligence budget of the United States government -- all generated by the effort to detail and sell information about our private lives," Rockefeller adds.

[Related: FTC Sends Warning Letters to 10 Data Brokers]

Privacy concerns have ebbed and flowed with the rise of the Internet for decades now, but the backlash against data collection has grown more recently as consumers wake up to the reality that their personal information is being bought and sold as a commodity. Former NSA contractor Edward Snowden's revelations about the wide and almost unfathomable reach of the federal government's surveillance apparatus has only stoked these flames of discontent.

Recent reports from the likes of CBS' news magazine "60 Minutes" are shining fresh light on data brokers as well (see video below). During that featured report, Federal Trade Commissioner Julie Brill says "your smartphones are basically mini tracking devices" that supply "the kind of information that really talks about who you are on a day-to-day basis."

That data may include information like when someone comes home or leaves, the places or establishments they frequent and when and where they swipe their credit cards to make purchases.

"I think most people have no idea that it's being collected and sold and that it's personally identifiable about them, and that the information is basically a profile of them," Brill says. "Consumers don't know who the data brokers are. They don't know the names of these companies."

Caught in the Cross-Hairs of the FTC

By flying under the radar, data brokers have largely been able to keep consumers at bay. The sheer volume of them, which easily number in the thousands, confuses consumers and matters of privacy all the more.

"When you're collecting across billions of data points, regardless of its accuracy, there's going to be groups of individuals behaving the same way."

-- Adam Kleinberg, CEO of Traction

The largest of these companies -- Acxiom, Datalogix, Epsilon and Experian -- are bridging together data from the online and offline worlds and selling it to the likes of Facebook, Twitter and others to enhance their respective ad products. The general approach is to group and categorize consumers for marketers' online ad targeting efforts. Programmatic ads are then sold and targeted based on these profiles, which the industry insists are anonymous and not personally identifiable.

Regulators and legislators across the political spectrum are making it a top priority to investigate these data brokers and enact laws that could curtail their way of business. But as more troubling details about the operation and seemingly unrestricted reach of these data brokers come to the surface, it's unclear what can or will be done to rein in their most damning practices.

[Related: Big Data Brings Big Privacy Concerns]

Daniel Kaufman, deputy director for the FTC's Bureau of Consumer Protection, says the agency is currently studying nine data brokers. "They collect an enormous amount of data and they are not consumer-facing," he said at last week's GigaOm Structure Data conference in New York City.

"How are they getting their data? How do they make sure it's accurate? Who are they sharing it with?" Kaufman says. The FTC takes law-enforcement actions, and it doesn't create regulations. However, he adds that "the commission has been supportive of legislation that would support or improve the transparency of data brokers."

Getting to Know You

The how, when and where of data collection may be perceived by many as nefarious, but the real debate begins over why. "Quite simply, in the digital age, data-driven marketing has become the fuel on which America's free market engine runs," the Digital Marketing Association wrote to members of Congress in 2012. That generally sums up the view of almost marketer today, and the sentiment is even more on point and agreed upon in the world of real-time marketing on social media.

"It's become an essential part of the marketing mix," says Adam Kleinberg, CEO of Traction, an advertising and interactive agency in San Francisco. Data brokers are "becoming increasingly important because the way digital media is being purchased is moving toward the robots. Programmatic advertising and programmatic media buying is using tools that automate the process," he says. "You enhance the targeting efficiency by leveraging that data. It's just gotten to the point in the past few years where 30 to 40 percent of media is purchased that way."

These profiles are directional and optimized behaviorally, Kleinberg says. The cookies that follow us around the Internet are being used to index us based on behaviors such as what we search, visit, click on or buy. "If you actually saw your data you'd think 'wow, these people don't know me at all,'" he says.

"The power of the data in certain circumstances is in the massive quantity and patterning that is possible. When you're collecting across billions of data points, regardless of its accuracy, there's going to be groups of individuals behaving the same way," Kleinberg adds.

"There is sensitive data that is collected and sold on you... What's new is this big data that is being collected and cross referenced with those things," he says. "The reality is that most of this big data is simply being used anonymously to better target you with an ad."

Can Marketers Police Themselves?

While he freely admits "the ability to look at that individual data is a little scary," he adds that "anyone who's buying digital media today is buying data."

From that the debate usually pivots around the promise of self-regulation versus the need for legal protections and regulations. Industry groups like the Internet Advertising Bureau and the Network Advertising Initiative have already developed standards and best practices which member companies must adhere to, but it appears unlikely that will remain their exclusive responsibility. Regulatory agencies and elected officials aren't subscribing to simple notion that the ends justify the means. Legislation could be on the horizon as they aim for a middle ground.

Sharing the view of the industry at large, Kleinberg says he thinks the responsibility should come from within because regulators don't have a deep understanding. "I think that the industry organizations are actually taking it very seriously and putting together standards that accommodate reasonable privacy restrictions like allowing people to opt out," he says.

"I think consumers care less than we think in the moment. They care in the abstract sense," Kleinberg says. "I can't tell you of an example where data has been abused."

To embolden the case for self-regulation, the industry needs to do more to explain what data means, Kleinberg adds. "The terms data and big data get lumped together as this big sinister beast and a lot of it is not innocuous ... it's anonymized by obscurity," he says. "We should not rush to judge all of it without understanding that nuance."

CIO.com Senior Writer Thor Olavsrud contributed to this report from New York City.

Matt Kapko covers social media for CIO.com. Follow Matt on Twitter @mattkapko. Email him at mkapko@cio.com Follow everything from CIO.com on Twitter @CIOonline and on Facebook.