

Anonymous, Social, Security

SA Evan C. Patterson

FBI - Charleston

West Virginia Office of Technology

The FBI does not support, condone or recommend any specific product, website, or company

لا إله إلا الله محمد رسول الله



SO



Thursday April 21, 2011, Ahmad F Al-Shagra

AlArabiya.net Hacked...Again

LOCKHEED MARTIN



BART
ba



Why the Hype?

- 📖 According to Symantec:
 - 📖 431 million victims of cybercrime last year
 - 📖 That only accounts for 24 countries
 - 📖 **That's 14 adults every second**

More Hype

- 📖 According to Ed Cohen, VP at SonicWALL
 - 📖 1 out of 4 computers infected with malware
 - 📖 10 million computers infected per month
 - 📖 250,000 computers added to botnets per month

Hackers leak data of Goldman Sachs CEO



By: Elinor Mills

SEPTEMBER 27, 2011 1:00 PM PDT

Print E-mail

Recommend

26

Tweet

56

+1

2

Share

3 comments

Hackers today released personal information for Goldman Sachs Chief Executive Officer Lloyd Blankfein.

The document, posted to the [Pastebin Web site](#), includes the CEO's age, recent addresses, details of litigation he has been involved in, as well as registration information for businesses, but no sensitive information such as financial data.

Goldman Sachs representatives did not immediately respond to a call seeking comment.

A group using the handle "CabinCr3w" took credit for the data dump, but did not say why Blankfein was targeted. Goldman Sachs benefited from the U.S. government's bailout of insurance giant American International Group and is accused of practices that contributed to the economic crisis.

On Monday, CabinCr3w [released information about a New York police](#)

[officer](#) who is seen in videos spraying pepper spray into the faces of women protesters who are penned behind a police barricade net at the "Occupy Wall Street" demonstrations. The officer, identified as Deputy Inspector Anthony Bologna via videos and close-up photos of his face and name on his badge, appears to walk over to the group of women and spray them directly in the face unprovoked.

A case of false arrest and civil rights violations is pending against Bologna in a claim brought by a protester involved in the 2004 demonstrations at the Republican National Convention, [The Guardian reported](#).

New York Police representatives have not responded to a CNET request for comment on the pepper spray allegations, but told The New York Times that the pepper spraying was appropriate and alleged that the video was edited, a claim that legal advocacy group USLaw.com, which analyzed the video in slow motion, [denies](#).

In a Tweet yesterday, CabinCr3w says "To the people asking...we are part of anonymous [SIC] just a group of like minded people taking on the world."



Lloyd Blankfein, chief executive of Goldman Sachs, is the latest target of hackers leaking personal information.
(Credit: [Goldman Sachs](#))

Microsoft halts another botnet: Kelihos

By: [Elinor Mills](#)

SEPTEMBER 27, 2011 11:15 AM PDT

[Print](#) [E-mail](#)[Recommend](#)

10

[Tweet](#)

72

[+1](#)

2

[Share](#)[6 comments](#)

Microsoft has put a halt to the Kelihos botnet and is accusing a Czech resident of hosting the botnet and using it to deliver spam and steal data, the company said today.

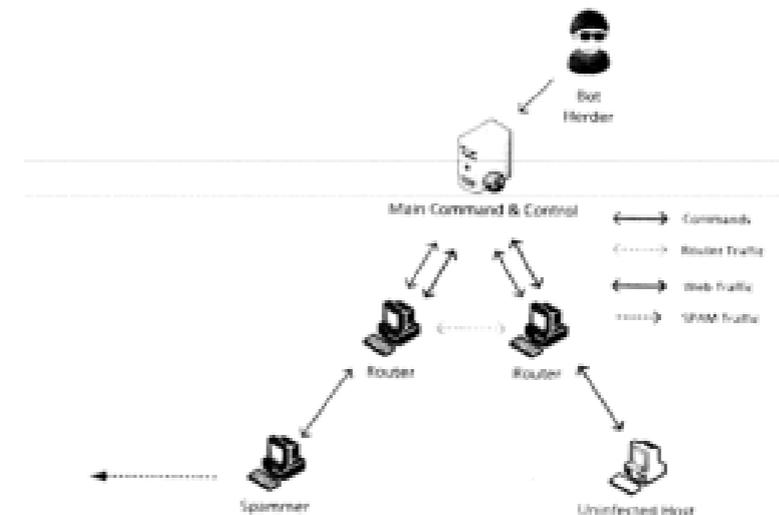
Kelihos, also known as "Waledac 2.0" after a previous botnet that [Microsoft shut down](#) last year, comprised about 41,000 infected computers worldwide and was capable of sending 3.8 billion spam e-mails per day, according to Microsoft.

The complaint filed last week in the U.S. District Court for the Eastern District of Virginia accuses Dominique Alexander Piatti, Dotfree Group SRO and John Does 1-22 of infecting victim computers with malware to create the Kelihos botnet, using it to send unregulated pharmaceutical and other spam, harvest e-mails and passwords, conduct fraudulent stock scams and, in some cases, promote sites dealing with sexual exploitation of children.

Meanwhile, subdomains were allegedly used to infect [Mac](#) computers with MacDefender scareware, according to the complaint. Piatti could not immediately be reached for comment.

In addition to filing complaints, Microsoft also is using a relatively new tactic of filing restraining orders to get court permission to sever the connections between the botnets and the individual infected computers, known as "zombies." This stops the botnet from continuing to operate and grow.

Microsoft also plans to work with ISPs and Community Emergency Response Teams (CERTs) to help clean up computers that were infected and used in the botnet. As part of that process, the Microsoft Malware Protection Center will add the Win/32 Kelihos family in a second release of the [Malicious Software Removal Tool](#) later today.



This image from the complaint illustrates how a bot herder uses a command-and-control server to communicate with infected computers via routers. (Credit: Microsoft)

Criminal Classifieds: Malware Writers Wanted



Hello there! If you are new here, you might want to **subscribe to the RSS feed** for updates on this topic.

You may also **subscribe by email in the sidebar** ➔

1

tweet

retweet

The global economy may be struggling to create new jobs, but the employment outlook for criminally-inclined computer programmers has never been brighter.

I've spent some time lurking on shadowy, online underground forums, and lately I've seen a proliferation of banner ads apparently placed by criminal gangs looking for talented programmers to help make existing malware stealthier and more feature-rich.

Долгосрочное
сотрудничество
работаем более 2х лет

от 2000\$
в месяц

Many of the ads highlight job openings for coders who are skilled in devising custom “crypters,” programs designed to change the appearance of known malware so that it goes undetected by anti-virus software. Anti-virus signatures are based on snippets of code found within known malware samples, and crypters can try to help hide or obfuscate the code. When anti-virus firms update their products with the ability to detect and flag files that are shrouded by this layer of obfuscation, malware writers tweak their creations in a bid to further evade the new detection mechanisms.

The composite banner ad pictured above is a solicitation from a crime gang that offers a base salary of \$2,000 per month in exchange for a “long-term partnership” creating crypters that include customer support. The ads lead to a sign-up page (below) where interested coders can leave their résumé and contact information, and state why they think they are qualified for the position.

'War Driving' Cybergang Indicted in High-Tech Business Theft

Sep 22, 2011 | 1:45 PM ET | By Paul Wagenseil, SecurityNewsDaily Managing Editor

Tweet

5

Like

25

SHARE



Office break-ins. The digital theft of hundreds of thousands of dollars. And a black Mercedes cruising the rainy city streets, equipped with the latest wireless technology to crack into corporate Wi-Fi networks.

This real-life high-tech thriller **first came to light in April**, when Seattle cops began to suspect two local men of pulling off dozens of digital burglaries.

Facebook Hacking Tool Clones Other People's Friends, Steals Their Profiles

Sep 14, 2011 | 3:10 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet

18

Like

356

SHARE



A free hacking tool called Facebook Pwn may turn your friends into enemies. Credit: Facebook

A new Facebook hacking [tool](#) could turn your closest friends into your worst enemies.

The tool, called "Facebook Pwn," lets **Facebook criminals** — and everyone else — steal personal profile information from any target of their choice on the massive social network. That's the end result, but it's the sneaky process you have to watch out for.

Anyone Play Angry Birds?

Cybercriminals Hack 'Angry Birds' Gift Shop to Attack Fans

Sep 16, 2011 | 11:35 AM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet 12 Like 32

SHARE



A site selling Angry Birds souvenirs was rigged with malware. Credit: Rovio

Playing too many games of "Angry Birds" can be dangerous to your productivity, and of course to all those birds catapulting erratically through the sky. It seems as though searching for souvenirs related to the wildly popular mobile phone game can also be just as threatening.

Internet crooks rigged an online shop selling "Angry Birds" merchandise with malicious software and downloadable files. Items such as an "Angry Birds Rubber Squeeze Toy" or an "Angry Birds Logo Home Button Sticker for iPad," were embedded with corrupt software that would infect users' computers and smartphones if purchased.

Love Thy Neighbor

Facebook Helps Man Steal \$57,000 from Neighbors

Aug 15, 2011 | 2:40 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

[Tweet](#) 15 [Like](#) 187

SHARE



Be careful what personal details you post on Facebook, they could give a criminal enough to rob you blind. Credit: Dreamstime

Can I Borrow \$7?

How to Become a Cybercriminal for Only \$7

Sep 22, 2011 | 12:24 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet 18 Like 52

SHARE



For about \$7, you too can be a cybercriminal. Credit: G Data Software

How much cash do you have on you right now? If it's \$10, you could spend it on a few snacks, less than a quarter-of-a-tank of gas or maybe an album on iTunes. Or you could enter the shady, soulless world of international cybercrime.

A botnet kit called "Aldi Bot" appeared about three weeks ago in underground forums, and has been selling for five Euros (about \$7). The kit allows its buyers to join ranks with an existing **botnet**, a linked network of compromised computers used to carry out large-scale online attacks.

Military Health Care Breach Exposes 5 Million Patient Records

Oct 3, 2011 | 11:12 AM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet

2

Like

SHARE



Credit: The Planet via Flickr

A data breach at a military health care provider may have exposed the personally identifiable and confidential information of 4.9 million patients.

The breach affected Science [Applications](#) International Corporation (SAIC), a McLean, Va.-based medical research company, and affected patients who received care from 1992 through Sept. 7, 2011, in military treatment facilities (including [clinics](#) and [hospitals](#)) in the San Antonio, Texas area through TRICARE, a health



SECURITY

People Who Get Malware Also Get Mugged More Than Usual

Our [Lifehacker AU](#) comrades point out this interesting fact from Norton's latest Cybercrime report: People who fall victim to malware are statistically more likely to be mugged in real life too. Interesting.

BY JASON CHEN 

SEP 8, 2011 11:00 AM

Share

+1

25,415  58 

Turning on Each Other

Facebook Hacking Tool Hacks Hackers

Sep 7, 2011 | 1:45 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet 11

Like 63

SHARE



facebook

Three tools designed to help people hack Facebook accounts actually contain malware that attacks the would-be hackers who download them. Credit: Facebook

A case of criminal irony: Tools built to help hackers break into Facebook accounts have been found hiding malware that infects the [computers](#) of the would-be criminals who download them.

The security firm [Bitdefender](#) detected three separate tools in the past two days, all of which promise fledgling Facebook fraudsters an easy and free way to steal people's passwords and gain access to their photos.



ANONYMOUS

Because none of us are as cruel as all of us.

WHAT IS - THE PLAN .ORG

ONE YEAR. THREE PHASES. A WORLD OF CHANGE.



EXPECT US.

ENTER NEW?

#5 Anonymous - É tempo para voar! [Spanish]



Empezamos a tomar las decisiones de que hacer y que no hacer

What is Anonymous? What is "The Plan"?



Anonymous

- 📖 Started on 4chan.org
- 📖 Became well-known in 2008 with Project Chanology
 - 📖 Against Scientology - DDoS, Calls, Faxes, etc
- 📖 “Not One Person”
- 📖 “No Leadership”

Epilepsy Foundation

- 📖 March 2008
- 📖 Flashing computer animations injected into forum to trigger migraines and seizures
- 📖 Mostly harassment, not “hacking”
 - 📖 Internet Griefers

Australian Government

- 📖 Feb. 2010
- 📖 DDoS Australian Government websites
- 📖 In response to country wide internet filtering
- 📖 Peak Bandwidth under 17Mbps
 - 📖 Typical DDoS now is 4Gbps some reach 49Gbps

Iranian Elections

- 📖 June 2009
- 📖 Setup Anonymous Iran a website to support the Iranian Green Party
- 📖 Provided resources including instructions to defeat government filtering and censorship
- 📖 Missing Persons Page
- 📖 To support free speech

Operation Payback

- 📖 September 2010
- 📖 Related to Operations Avenge Assange/Bradical
 - 📖 In retaliation for stopping payment processing and webhosting for wikileaks
 - 📖 Targets: Amazon, PayPal, Mastercard, Visa

HBGary Federal

- 📖 February 2011
- 📖 In retaliation for threatened release of Anonymous usernames/identities
- 📖 Hacked their public website, internal emails, released government contracts, etc
- 📖 Hacked CEO's twitter account and posted home address and social security number

Operation BART

- 📖 August 2011
- 📖 In retaliation for BART shutting down cell phone service in certain stations to prevent protestors from communicating
- 📖 Released semi-private nude photos of BART spokesman
- 📖 Defaced mybart.org and released email addresses of registered users

LOIC

- 📖 Low Orbit Ion Cannon
 - 📖 Developed by 4chan affiliated hackers
 - 📖 Free Download
 - 📖 Used for DDoS
- 📖 Are users really “Anonymous”
 - 📖 Most do not use anonymization software
 - 📖 Most are “low skilled” “hackers”
 - 📖 Wannabe

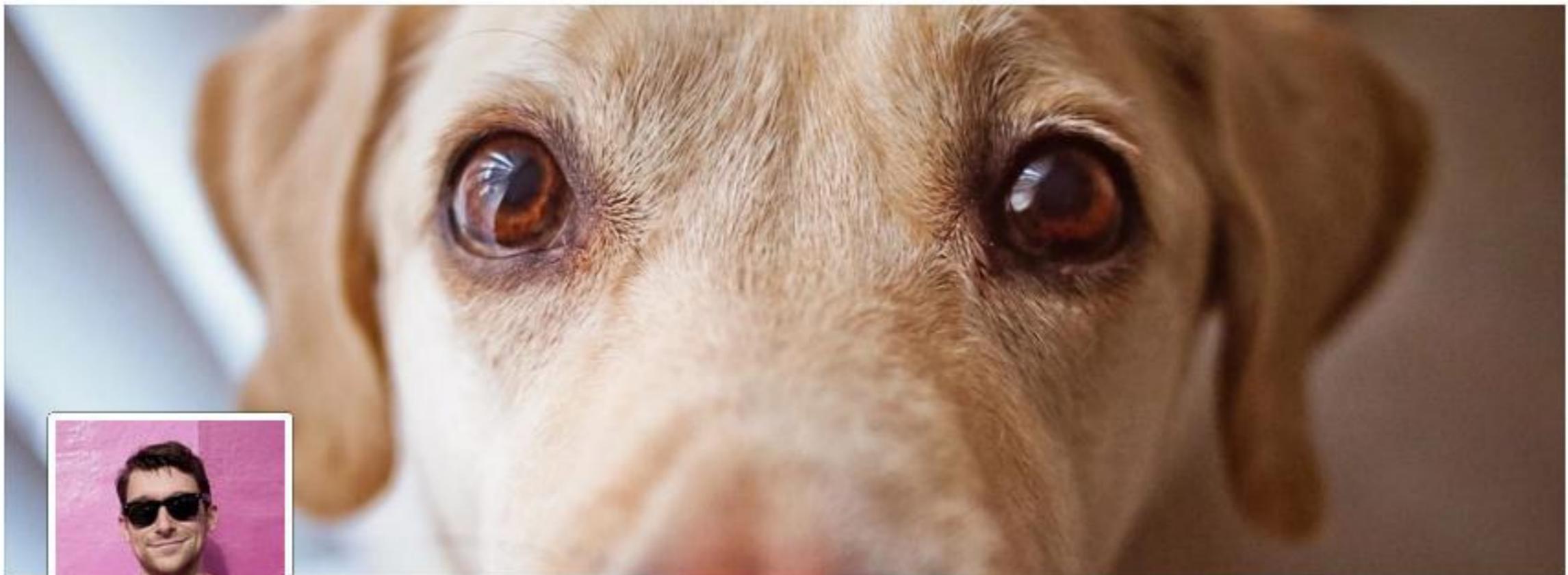
LulzSec

- 📖 Connections to, but not affiliated with Anonymous
- 📖 Formed May 2011
- 📖 Embarrassing companies into better security “for the Lulz”
- 📖 Hacked: Fox.com, Sony, PBS, Nintendo, pron.com, writerspace.com, InfraGard Chapter Sites, NHS, senate.gov, cia.gov, Arizona DPS, AT&T, etc

Facebook's Timeline

Your Cover

Fill this wide, open space with a unique image that represents you best. It's the first thing people see when they visit your timeline.



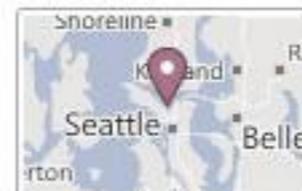
Matt Brown

[Update Info](#)

[View Activity](#)



- Communication Designer at Facebook
- Studied English at Indiana University
- Lives in San Francisco, California
- Married to Tiffani Jones Brown



4 ▾

Your Stories

Share and highlight your most memorable posts, photos and life events on your timeline. This is where you can tell your story from beginning, to middle, to now.

Status Photo Place     

What's on your mind?

 **Matt Brown**
August 29 

Last Weekend / SF Moma (16 photos)



Recent Activity

 Matt likes Mountain Biking.

 Matt subscribed to Tom Watson's updates.

 **Matt Brown**  
August 21

2nd Anniversary Backpacking — Point Reyes (3 photos)



Like · Comment

 **Matt Brown** became friends with Nicholas Felton.
August 11

 **Nicholas Felton**
 Co-workers at Facebook
[See friendship](#)

Your Apps

The movies you quote. The songs you have on repeat. The activities you love. Now there's a new class of social apps that let you express who you are through all the things you do.



Matt Brown completed a run.
August 6 via RunKeeper

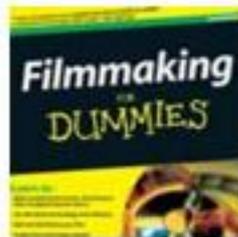
3.61 miles

Duration: 38'27" | Pace: 10'39"/mile

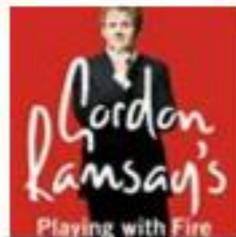
Like - Comment

Kobo
August

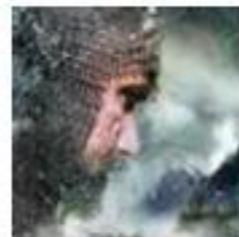
Recently read



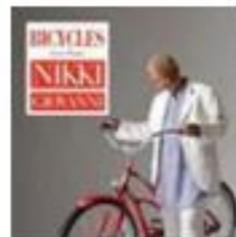
Filmmaking For Dummies, 2nd Edition
Last read on Thursday



Playing With Fire
Last read on Tuesday



Fall of Thanes
Last read on Tuesday



Bicycles: Love Poems
Last read on Monday



Netflix
August

Movies Watched



Super Size Me

Documentary filmmaker Morgan Spurlock puts his touch...



Exit Through the Gift Shop

The story of how an eccentric French shop keeper...



Spotify
August

Top Album



Keegan DeWitt

Thunder Clatter

Thunder Clatter — 47 plays

Colors — 43 plays



Matt Brown watched 7 movies on Hulu.
August 4



Nike+ GPS
August 2011

Longest Run

6.32 miles

Duration
1:38:27

Avg. Pace
10:39/mile

Facebook Defends Getting Data From Logged-Out Users

Article

Comments (33)



Email



Print



Like

618



Send



+ More



Text

By Jennifer Valentino-DeVries

Facebook on Monday defended its practice of gathering data from “Like” buttons even after users have logged out, saying that the collection is part of a system to prevent improper logins and that the information is quickly deleted.

The comments from the social-networking giant come after Australian technologist [Nik Cubrilovic](#) published findings showing that unique identifiers were sent from “Like” buttons when users were not logged in, raising questions about the privacy implications of Facebook’s vast presence on the Web.

“Even if you are logged out, Facebook still knows and can track every page you visit,” Cubrilovic wrote in a blog post about the issue. “The only solution is to delete every Facebook cookie in your browser, or to use a separate browser for Facebook interactions.”

Here's how the Facebook data collection works: When you log in to Facebook or visit Facebook.com without logging in, the site places small files called “cookies” on your computer. Some of these cookies remain on your computer even after you log out, and then whenever you visit a site that connects to Facebook – such as those with a “Like” button – information from those cookies is sent back to Facebook, providing a record of where you’ve been on the Web.

Facebook acknowledges that it gets that data but says it deletes it right away. The company says the data is sent because of the way the “Like” button system is set up; any cookies that are associated with Facebook.com will automatically get sent when you view a “Like” button.

“The onus is on us is to take all the data and scrub it,” said Arturo Bejar, a Facebook director of engineering. “What really matters is what we say as a company and back it up.”

In a statement, a Facebook spokesman said “no information we receive when you see a social plugin is used to target ads.”

Facebook allegedly promises to fix logout cookies issue

Posted on 27 September 2011.



The Facebook tracking cookies issue revealed yesterday has, expectedly, created quite a stir in the security community.

The company went into damage control mode and repeated the claims made by one of its engineers: "Facebook does not track users across the web."

"Instead, we use cookies on social plugins to personalize content (e.g. show you what your friends liked), to help maintain and improve what we do (e.g. measure click-through rate), or for safety and security (e.g. keeping underage kids from trying to signup with a different age). No information we receive when you see a social plugins is used to target ads, we delete or anonymize this information within 90 days, and we never sell your information."

"Specific to logged out cookies, they are used for safety and protection, including identifying spammers and phishers, detecting when somebody unauthorized is trying to access your account, helping you get back into your account if you get hacked, disabling registration for a under-age users who try to re-register with a different birthdate, powering account security features such as 2nd factor login approvals and notification, and identifying shared computers to discourage the use of 'keep me logged in'."

Facebook Privacy



TOP STORIES



ALWAYS UP TO DATE GUIDE

The Always Up-to-Date Guide to Managing Your Facebook Privacy

BY WHITSON GORDON JUN 21, 2011 8:00 AM

Share +1 Like 5K 88,134 33

Keeping your Facebook info private is getting harder and harder all the time—mostly because Facebook keeps trying to make it public. To help you out, we've created a comprehensive guide to keeping your Facebook locked down and in your control, and we're going to keep it updated whenever Facebook decides to add a new feature or



Facebook Privacy

📖 Changes Often

📖 Therefore Check Often

📖 “View As”

📖 Online Guides

📖 [Facebook.com/Security](https://www.facebook.com/Security)

📖 Lifehacker Guides



The image shows a screenshot of a Lifehacker article. At the top, the Lifehacker logo is visible in green. Below it is a photograph of a blue door with a white house number '35', a brass doorplate that says 'facebook', and a white sign that says 'DO NOT DISTURB'. The article title is 'The Always Up-to-Date Guide to Managing Your Facebook Privacy' by Whitson Gordon, dated June 21, 2011. The article text begins with 'Keeping your Facebook info private is getting harder and harder all the time—mostly because Facebook keeps trying to make it public. To help you out, we've created a comprehensive guide to keeping your Facebook locked down and in your control, and we're going to keep it updated whenever Facebook decides to add a new feature or...'. There is also a Samsung logo and a smartphone image in the bottom right corner of the article preview.

Facebook's New Timeline: Important Privacy Settings to Adjust Now

Facebook's new Timeline has the potential to expose status updates and wall posts from years ago. Here's how you need to update your privacy settings before you or Facebook publishes your Timeline.

By Kristin Burnham
Thu, September 29, 2011

Like 2K

+1 54

4 Comments

[CIO](#) — If you care to keep your past in the past, Facebook's new version of the profile, called [Timeline](#), makes that a little more difficult.

238

Tweet

63

Share

0

Reddit

1

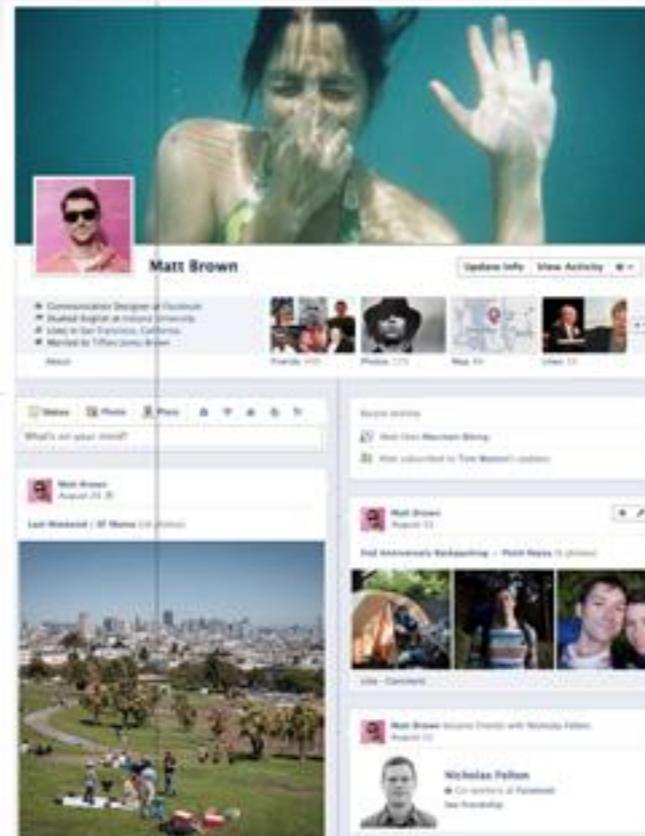
Digg

0

Submit

30

Email



Similar to this Article

Everyone Hates Facebook, A Pictorial

Facebook Privacy: Uncovering 5 Important Settings

Facebook's New Friend Lists: 6 Things You Need to Know

With Timeline, every status update, wall post and photo ever posted since the day you joined Facebook becomes easily searchable to you and your friends. For many—early adopters especially—dredging up the past for all to see can be a privacy nightmare.

When your Facebook account is migrated to the new Timeline—which Facebook started rolling out today—you'll have one week to make any adjustments to your past posts and privacy settings before your Timeline will go live for everyone to see. You can publish it yourself anytime within the five-day waiting period.

What To Do

📖 Learn

📖 Decide

📖 Implement



Learn

-  Research Online
-  Attend Conferences (Check)
-  Talk with Smart People

Decide

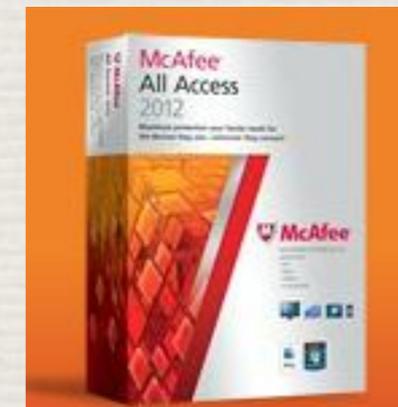
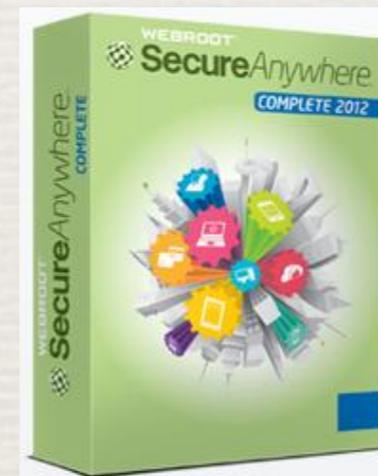
- 📖 Think First, Post Later
- 📖 Would I Want My Grandma to See This?
- 📖 Watch Your Kids
- 📖 Decide What You Want Public, Don't Just Accept the Defaults

Implement

- 📖 Install Antivirus and Anti-Malware
 - 📖 There are free versions available
- 📖 Monitor Your Activity and Your Kid's Activity
- 📖 Check Your Settings Periodically
- 📖 Update Your Software Regularly (not just patches)
- 📖 Change Your Passwords
- 📖 You Don't Have to be a Mechanic to Know Your Car is In Trouble

Suite Software

- 📖 Antivirus, Firewall, Spam Filtering
- 📖 Multiple Devices (including phones)
- 📖 Multiple Products (do your research)





US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

[Security Publications](#)

[Alerts and Tips](#)

[Related Resources](#)

[About Us](#)

[GFIRST](#)

Search:

[GO](#) [customize](#)

Information For

[Technical](#)

[Non-Technical](#)

[Government](#)

[Control Systems](#)

Cyber Security Tips

Cyber Security Tips describe and offer advice about common security issues for non-technical computer users.

[Sign up](#) to receive these security tips in your inbox.

[RSS](#)

[+ MY Y!](#)

<http://www.us-cert.gov/cyber/>

<http://is/s>

<http://ww>

<http://ww>

lifehacker

TOP STORIES

KNOW YOUR NETWORK
The Complete Guide



Let's Remember to Parent

Dad Sues Facebook Over Preteen Daughter's Racy Pics

Sep 8, 2011 | 11:51 AM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet

3

Like

62

SHARE



A father is suing Facebook over racy photos his 12-year-old daughter posted. Credit: Facebook

A father in Northern Ireland is suing Facebook for allowing his 12-year-old daughter to post sexually explicit photos of herself online.

The **BBC** reported that the man, whose name remains undisclosed, said Facebook is "guilty of negligence" for not preventing the girl from posting **sexually explicit photos** of herself. By letting her bypass its age restrictions, Facebook created "a risk of sexual and physical harm" to the girl, her father alleged in a Belfast court on Monday (Sept. 5).

Government Involvement

Germany vs. Facebook: Like Button Declared Illegal, Sites Threatened With Fine



📅 August 19, 2011

Written by: **Frederic Lardinois**

Germany has a long tradition of using laws to protect its citizen's privacy. Home owners, for example, can ask Google to pixelate their houses in [Street View](#) (maybe so that their garden gnomes can stay incognito?). Facebook's facial recognition feature has also [come under fire](#) in recent weeks. The latest target of Germany's privacy advocates is Facebook's 'like' button („Gefällt mir," in German). Thilo Weichert, the head of the Independent Centre for Privacy Protection of the northern German state of Schleswig-Holstein, [argues](#) that Internet sites based in his state that use the 'like' button are [illegally sending this data to Facebook](#), which in turn uses it to illegally create a profile of its users web habits.

Updated: German websites based in the state of Schleswig-Holstein have until the end of September to remove [Facebook's](#) 'like' button or face a fine of up to 50,000 Euro.



Anonymous Involved

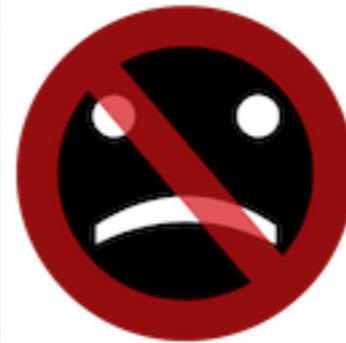
- 📖 Probably not “official” Anonymous
- 📖 Threatening to takedown Facebook



Internet Shame Insurance

📖 Google Chrome Extension

📖 Pops up a message to remind you who can see your post



Internet Shame Insurance

Platform: Windows, Mac, and Linux with [Google Chrome](#)

Price: Free

Author: [Adam Pash](#)

License: [GNU Public License](#); Source available on [github](#)

[Click Here to Download and Install](#)

Insurance



LIFEHACKER CODE

Save Yourself from
Weiner-Caliber Online
Embarrassment with
Internet Shame
Insurance

BY ADAM PASH  JUN 9, 2011 2:05 PM

[Share](#)   Like  75,863  64 

I Have a Mac!

Insider: Mac Trojan Hides in Fake Adobe Flash Installer

Sep 27, 2011 | 3:23 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer



Tweet

7

Like

12

SHARE



A tricky new Mac Trojan is hiding as a Flash Player installer. Credit: Apple

Back In a "flash," Mac users can unknowingly download a harmful Trojan.

home that comm mom The Trojan, called "Flashback," has been spotted hiding inside phony Adobe Flash Player installers, and if downloaded, it can wreak havoc on Apple's OS X operating system, according to the security firm **Intego**, which discovered it.

Call Law Enforcement

- 📖 It is important to call your bank (if it involves them)
- 📖 Let someone know in LE
- 📖 Let us decide what is investigated

CALLING FOR HELP

When cybercrime strikes, **less than half** of all victims call their financial institution or the police and just over **a third** contact the website owner or email provider.

Who victims contact





INTERNET CRIME COMPLAINT CENTER

... an FBI - NW3C Partnership

[Home](#) [File a Complaint](#) [Press Room](#) [About IC3](#) [Contact Us](#)

Welcome to the IC3

The Internet Crime Complaint Center (IC3) is a partnership between the [Federal Bureau of Investigation \(FBI\)](#), the [National White Collar Crime Center \(NW3C\)](#), and the [Bureau of Justice Assistance \(BJA\)](#). [Read more >>](#)

Situational Alert

26 AUGUST 2011. In light of Hurricane Irene, the public is reminded to beware of fraudulent emails and websites purporting to conduct charitable relief efforts. To learn more about avoiding online fraud, please see "Tips on Avoiding Fraudulent Charitable Contribution Schemes" at: <http://www.ic3.gov/media/2011/110311.aspx>

Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint.

Search

▶ [FAQs](#)

▶ [Legal](#)

▶ [Disclaimer](#)

▶ [Privacy Notice](#)

▶ [Protect Yourself](#)

▶ [Internet Crime Prevention Tips](#)

▶ [Internet Crime Schemes](#)

▶ [Public/Private Alliances](#)

▶ [Site Map](#)



**Protect Yourself
With The Latest IC3
Consumer Alerts!**

▶ [Mass Market Fraud](#) 



▶ [IC3 Flyer](#) 



InfraGard

-  www.infragard.org
-  Free Membership
-  Good Networking
-  Sensitive Information

Questions

 SA Evan C. Patterson

 evan.patterson@ic.fbi.gov

 [304-340-9366](tel:304-340-9366)