



Global threat report


August 2011

Feature Article: Irish holidaymakers expose themselves to dangers.



Table of Contents

Irish holidaymakers expose themselves to dangers.....	3
Social Media and Political Certainties	3
PUAs: ESET’s Most Unwanted List.....	5
Mobile devices auto-import phonebook to Facebook.....	7
1000 days of Conficker	7
The Top Ten Threats	8
Top Ten Threats at a Glance (graph)	12
Annexe.....	13
About ESET	15
Additional resources.....	15



Irish holidaymakers expose themselves to dangers

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

One third of the Irish enjoy holiday gloating while another third prefer secret holiday destinations.

With the holiday season nearly over we wanted to know, how much of their holiday plans or activities the Irish reveal on social media? This security issue goes beyond announcing that your house will be empty in a certain period and thus inviting burglary. Lately, cybercriminals often contact their target's social media friends with some sort of financial scam that involves the holiday destination. (This is sometimes referred to as Londoning, though it's by no means confined to imaginary London, as explained here.)

Urban Schrott, ESET Ireland's cybercrime analyst comments: "Say someone posted on his Facebook profile that they're looking forward to their holiday in Lanzarote. Well, cybercriminals often check for such info on visible Facebook accounts and then they can easily fake an email seemingly from the account-holder and target some of their friends saying something like 'I was mugged in Lanzarote, please send me €500 to sort things out and get home,' with a request to transfer funds untraceably through Western Union. Scams like this appear credible, and are occurring all the time. With the location of the holiday made known, many more people fall for it and send money to their 'friend in distress', then are shocked to find the friend was never mugged and knows nothing about it."

In its latest survey ESET Ireland asked Irish computer users how much info they reveal on social media. One third of Irish adult

internet users never post their travel plans on a social media website. Almost 1 in 10 always post, while another 1 in 10 only allow certain friends to see the information. If we say the worst security offenders are those that tell everyone, well, there's only about 9% of those. But add to that another 13% that sometimes post, and 8% that only tell some friends, then nearly a third of respondents do reveal some info, therefore putting themselves and their friends at risk.

The full results of the survey are as follows:

(See the Annexe: Image 1)


Another interesting detail is that 11% of Irish males post before travelling but only 7% of Irish females, whereas only 9% of males and 16% of females post after they've returned home. And the people of Leinster, who scored highest in never posting and lowest in always posting of all regions, seem to be wisest in telling everyone it's nobody's business where they spend their holidays.

ESET Ireland recommends you behave safely online and try to filter information you disclose about yourselves so that the chance of the information being abused in any way is minimized.

Social Media and Political Certainties

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

An earlier version of this article was previously published in SC Magazine's CyberCrime Corner



The recent crime-wave in the UK, whether or not you believe it has some genuine basis in political activism (and it's hard to see how looting televisions and robbing the injured will eradicate injustice), may not be cybercrime as we have been accustomed to think of it, but it does have an IT dimension. Adding further items to the list of discomfoting ways to use social media, with Twitter and Facebook and even Blackberry Messenger used for communication between prospective participants, has also exposed inconsistencies in some political assumptions.

Thomas Mann once wrote, that everything is politics: and I think he was right: restricting the label "political" to the activities of those who have offices just off the Corridors of Power simply gives them leave to play in their own sandbox with a minimum of interference from those whose lives they regulate on so many levels. But that being so, it's not surprising that the ever-more-pervasive influence of the Internet on society is not always seen as a positive, and a single service (or even a single protocol) can be both a Good Thing and a Bad Thing.

The British government's sudden desire to co-opt Facebook, Twitter and RIM into a law-enforcement strategy is symptomatic of a realization that state perception of the validity of media freedom is not based on absolute values but on context. One nation's social threat is another's liberation movement. It seems that it's not only China but the Geek Peninsula (sic) that has trouble distinguishing between shutting down Blackberry Messaging and the Great Firewall of China.


Actually, there's nothing new here in principle. Messages relating to criminal activity can be carried as easily (if not as quickly) by snailmail, and postal carriers (like telephony providers) usually expect to be required to cooperate with law enforcement agencies at least some of the time: relatively few people get overly heated about defending the rights of

paedophiles or bombers. The real difference is in the immediacy of more recent social media in the age of the smart-phone. In fact, it's not just the immediacy, but the visibility of the media. And I don't just mean the fact that Twitter and Facebook are readily available practically anywhere to anyone with a smart phone (and if you have a Blackberry that extends the third leg of the tripod...)

Consider the humble SMS texting service: Twitter and similar SMS-based services haven't really extended the possibilities of the simple text much in terms of content: however, the volume of people who can be reached by a single text is revolutionary (just ask @LuzSec...) Even worse (as regards tweets and other posts that are "anti-you"), the whole online world can see the damage. I guess we'll see in due course whether conversations between the vendors in question and the UK's Home Secretary extend to the kind of routine interception of encrypted messages that some states have demanded from RIM, or will simply formalize interception on request (backed up by due legal process), possibly augmented an agreement to supply general intelligence that might precede such legal process.

It doesn't seem likely to me, though, that we'll see a more generalized Great Firewall of Great Britain in the near future: the services currently being discussed are probably too big and too popular for cheap, easy retrofitting with some kind of Killswitch of the kind Cameron Camp has discussed on the ESET ThreatBlog.

On the other hand, the combination of size and visibility does mean that it's harder for the major social networking providers to fall back on the "common carrier" argument ("we just carry messages, we don't police them...") used in the past by email providers. Massive misuse of the social media in pursuit of criminal activity is just too in-your-face to be ignored: consider, for example this more-or-less random and geographically



widespread selection of news items relating to arrests and/or court appearances in the UK.

Scottish youths arrested over Facebook 'riot' messages

- [Essex Police make Facebook 'riot incitement' arrest](#)
- [Web ban for teens accused of Facebook 'riot' page](#)
- [Pregnant mum charged with handling goods stolen in Birmingham riots \[the reference to incitement is later in the article\]](#)
- [England riots: teenager freed after encouraging vandalism on Facebook](#)
- [Facebook Plymouth Riot Arrests](#)
- [Glaswegian arrested for pro-riot Facebook posts](#)
- [Pair arrested in Llanelli for Facebook 'riot' posts](#)
- [UK police arrests 10 more over Facebook posts inciting riots](#)
- [Facebook arrest for Bream teen "inciting village riot"](#)

PUAs: ESET's Most Unwanted List


This month, our distinguished researcher Aryeh Goretsky wrote the paper [“Problematic, Unloved and Argumentative: What is a potentially unwanted application \(PUA\)?”](#) The following lines are an interview between Sr. Research Fellow David Harley and

the paper's author, talking about the content of it:

David Harley (DH): It seems to me that in spite of much increased public awareness in the last decade or so, people in general are not good at distinguishing between types of malware, and even the wider security community sometimes accuses us (AV specialists) of having pseudo-religious arguments about classification and taxonomy instead of implementing that 100% detection they think we should be able to provide. However, one issue that seems to come up pretty often on forums and in the press is this: given the risks from destructive malware, password stealers and so on, "possibly unwanted" seems both vague and lacking in drama. Does adware and such really matter that much? (Rhyming responses are not necessary.)

Aryeh Goretsky (AG): Actually, I'd say these types of programs are more an issue now than ever: It used to be anti-malware companies could make very binary decisions about whether a program was malicious or not. Classic computer viruses could be identified by their recursively self-replicating nature, Trojans by how they claimed to perform one set of actions but covertly performed others and the criminal gangs behind these programs could be similarly classified, as well. Today, the amounts of threats seen are magnitudes of order more than in previous decades, and the spectrum of these malicious codes—and the actors behind them—extends far beyond these easily-defined black-and-white categories to much grayer areas. We have to look at things like intent; potentials, possibilities and likelihoods of misuse; percentages of customers who may actually want to make use of such software and other criteria before deciding how to categorize such threats. (Rhyming response not given.)

DH: That makes sense to me, but then I've read the paper and I work in the industry. But for people who don't have those



advantages, it leads to another question. If PUAs do matter that much, why do some vendors flag PUAs by default and others make them optional?

AG: That can depend on a number of factors, such as the intended audience for the product (business, consumer or mixed), what threats the vendor emphasizes detecting in their product literature, requirements from their customers and so forth. In ESET's case, the decision about whether to detect potentially unwanted applications is placed in the hands of the customer because we believe it is ultimately their choice, not ours, as to whether such programs should be allowed on their computers. On the opposite side of the fence, an otherwise legitimate program may be bundled with a component that is a PUA, but prompt the customer as to whether or not it should be installed. So, providing the customer with a choice is a concept which exists for some PUA vendors, as well. Of course, there are PUAs which are hidden, integral to a program or otherwise do not allow the user to make a choice about installing them.

DH: You might think this is a slightly disingenuous question, given that I'm a director of the Anti-Malware Testing Standards Organization (AMTSO), but surely that creates a problem with product testing?

AG: Yes, it does. Because criteria for detection as potentially unsafe or potentially unwanted applications varies with the vendor, as well as default settings for detection in their anti-malware programs, a test set containing these types of applications can return very different results depending upon how the anti-malware programs is configured. There is also the question of how the tester interprets these results. If an object is flagged during testing as potentially being a threat instead of definitely being one, does that count towards detection? Or could it be classified as a missed detection or even a false


positive report?

DH: It's certainly an issue... In fact, there's an AMTSO guidelines document in preparation on selecting samples that will, hopefully, clarify things a little. (I'm supposed to be working on it this week, so glad of your input, as someone who's better acquainted with ESET product development than I am!) Do you think the PUA problem in general has grown in recent years?

AG: I *know* the problem has grown in recent years, largely from looking at the increased number of PUAs being listed in updates to ESET's threat signature database.

DH: Why do you think that is?

AG: Although the actions of potentially unsafe and potentially unwanted applications can be quite different from other types of malware, they typically have one trait in common: They are intended to make money for someone. Unlike some malicious activities which are unequivocally criminal, like botting a PC to make use of its resources, stealing sensitive information from it or ransom/blackmail-type scenarios, a legitimate software vendor might include a PUA component as a way of generating revenue. Be it a primary means or simply some supplemental income, which can be important for a software vendor as competition increases and revenue from licensing their product goes down. This gives the legitimate software vendor a way to underwrite continued development and maintenance for their software. This form of "sponsorship" might seem like a good deal to a software vendor, but it may also result in upset customers, depending upon the default installation options and behavior of the PUA.



Mobile devices auto-import phonebook to Facebook

If you downloaded the Facebook app for your mobile device, and just zipped through the install options (like users commonly do), did you know all your contacts could now be on your Facebook Contact list (formerly Phonebook) and can be datamined by Facebook? This is also disturbing if Facebook itself gets hacked and your phone contacts get stolen, giving significant access by malcontents to personal information about you and your contacts. Also, it would provide a larger incentive for bad actors seeking to harvest and sell your personal information to the highest bidder, now they'd have even more of your information (and others) in one fell swoop. Note that Facebook says the Contact list contents aren't necessarily publicly visible, stating, "Just like on your phone, only you can see these numbers."

If you choose later to opt out of having your mobile device phonebook sync'ed, you wouldn't be alone. The forums are rife with users trying to figure out how to easily disable the sync function on their specific mobile device. Some have even resorted to removing the app altogether and re-installing it without the feature enabled, some just give up. Clearly, steps could be taken by the Facebook mobile team to make it easier for the user to opt out later, though some suspect this is by design. After you manage to disable the sync feature on your device, you also would have to disable it on the Facebook.com site under your account. To do that, you can visit:

Account -> Edit Friends -> (Mobile graphic) Contacts

Then follow the link on the right side...

(See the Annexe: Image2.1)

... which will lead you to a page like:


(See the Annexe: Image 2)

Notice there is a reference to an iPhone, which wasn't used in this example, but no reference for how to do it on the device that was used. Also, notice the bit about friend suggestions becoming less relevant if you opt out? This means their algorithms would know less about you, so could predict with less precision who you might also want to friend. Advertising harvesters use similar language when attempting to target marketing efforts, and there's no small amount of business to be had feeding increasingly accurate information to a prospective high bidder.

1000 days of Conficker

Conficker is a special worm: 1000 days after his appearance, we are still talking about it. This month, it had been 1,000 days since the Conficker worm first appeared on November 21, 2008. Regarding this fact, [Aryeh Goretsky pointed on ESET Threat Blog](#) a special history trying to answer the most important question regarding Conficker: why is it that nearly three years later the Conficker worm, running "headless" without Command and Control (C&C), using a three year old exploit and dealt with by all current anti-malware software is still at the top of the malware ecosystem? (Story names are not the real ones)

John works as an administrator at a regional company, where he supports thousands of desktops across several states. I say support, and not manage or administer, because of the nature of John's environment: John's employer is a business that has grown by acquiring smaller companies. As a result the company has dozens –if not hundreds – of different networks,



computers, operating environments, best practices and standards for managing all of these. In other words, this is an enterprise-sized deployment of, well, workgroups. While they have made some inroads towards establishing universal standards, the organization's computer security is still a patchwork at best. For example, there is no centralized management of security. That coupled with the fact that some users still have administrative access to their PCs due to legacy software, means that employees can turn off or even uninstall their antivirus software at will.

And what does this mean for John? It means that his company's users have been infected with Conficker somewhere in their company every single day since the worm came out.

While there are technical issues that facilitate this pandemic, the underlying cause is not really technical: John's employer has not implemented the means to protect their employees because of the expense of installing a centralized management and security solution: such an implementation also has to factor the cost and inconvenience of replacing legacy programs and computers, and training employees on the replacement systems, in the current economic climate.

I agree that solving this particular problem will be very costly. Even using open source software, they are looking at a significant capital expenditure for deployment, and those costs are only going to increase with each acquisition. Of course, the sooner his company switches to a centralized management and security model, the better off they will be, especially when it comes to integrating acquisitions.

While one might have sympathy for John's employer and understand their desire to fight these hot spots rather than put out the forest fire due to the hit in profitability they'll take, there's one other aspect of John's employer I have not

mentioned.

It is in the healthcare business.

In the United States, that means they are subject to HIPAA rules. While HIPAA is not something we discuss very often because it is a complicated and specialized area, a worm traversing networks containing medical records for nearly three years seems like it would be the type of thing HIPAA was meant to address.

To read the whole blog post, visit [ESET Threat Blog](#).

The Top Ten Threats


1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.40%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this



isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (<http://www.eset.com/threat-center/blog/?p=94>; <http://www.eset.com/threat-center/blog/?p=828>) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at <http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun> useful, too.

2. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 4.22%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC subsystem and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lang=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third

quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: <http://www.eset.com/threat-center/blog/?cat=145>

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

3. HTML/Iframe.B.Gen

Previous Ranking: 5
Percentage Detected: 2.38%
Type of infiltration: Virus

HTML/Iframe.B.Gen is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

4. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 2.22%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely.



The file is run-time compressed using UPX.

The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

5. Win32/Sality

Previous Ranking: 3
Percentage Detected: 2.10%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:

http://www.eset.eu/encyclopaedia/sality_nar_virus_sality_aa_sality_am_sality_ah

6. HTML/ScrInject.B

Previous Ranking: 6
Percentage Detected: 1.79%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

7. Win32/Autoit

Previous Ranking: 8
Percentage Detected: 1.45%

Win32/Autoit is a worm that spreads via removable media, and some of its variants spread also thru MSN. It may arrive on a system as a downloaded file from a malicious Web site. It may also be dropped by another malware. After infecting a system, it searches for all the executable files and replace them with a copy of itself. It copies to local disks and network resources.

Once executed it downloads additional threats or variants of itself.

In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry.

8. Win32/PSW.OnLineGames

Previous Ranking: 4
Percentage Detected: 1.23%


This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Research team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at

[http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport\(Jan2009\).pdf](http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf)

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: n/a
Percentage Detected: 1.12%



It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

10. Win32/Ramnit

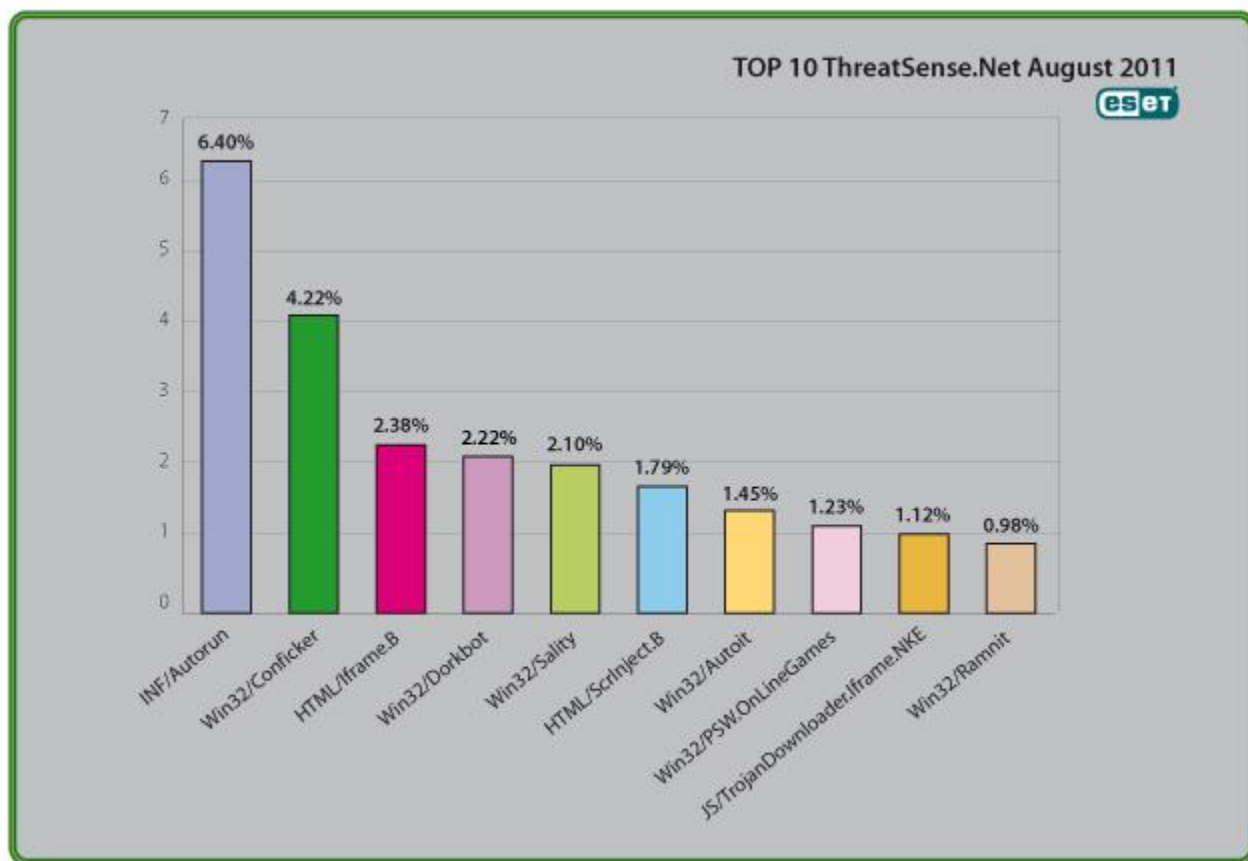
Previous Ranking: 41
Percentage Detected: 0.98%

It is a file infector. It's a virus that executes on every system start. It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotely to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.

Top Ten Threats at a Glance

(graph)

Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 6.40% of the total, was scored by the INF/Autorun class of threat.



Annexe

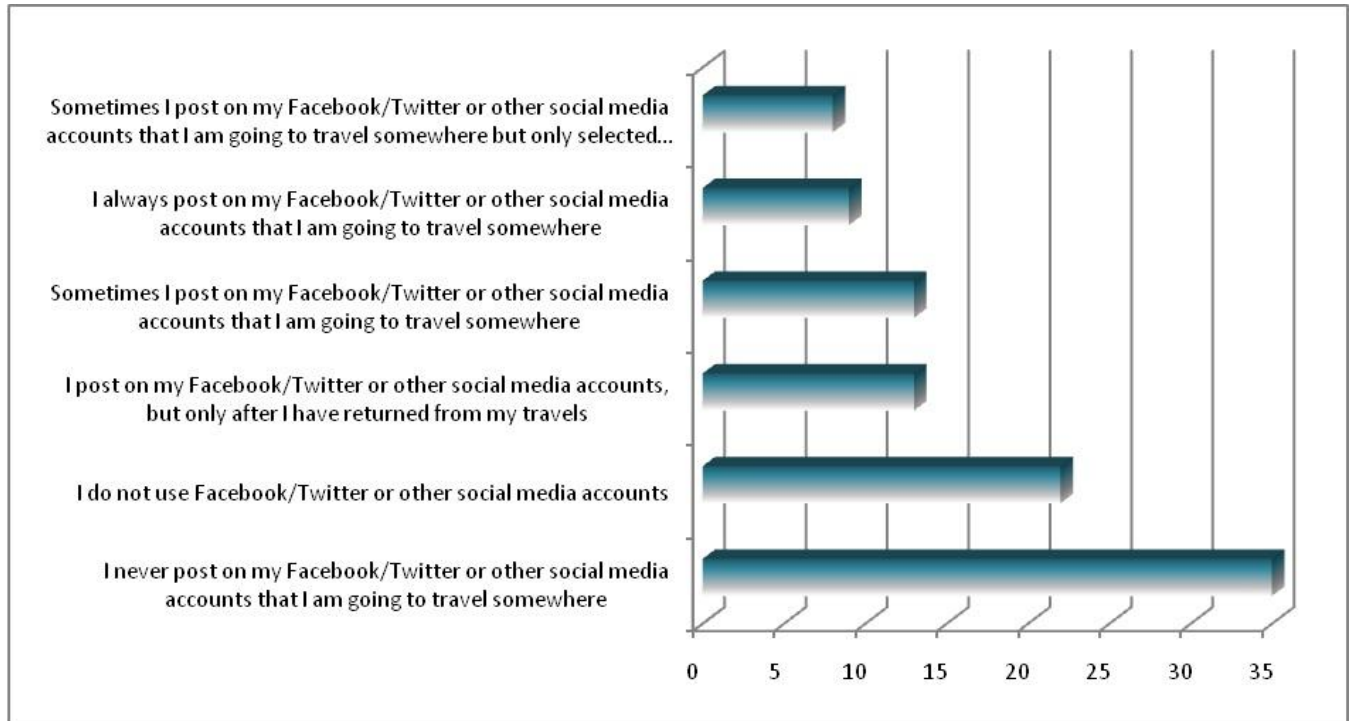


Image 1

Phonebook Contacts

Facebook Phonebook displays contacts you have imported from your phone, as well as your Facebook friends.

If you would like to remove your mobile contacts from Facebook, you need to disable the feature on your mobile phone and visit [this page](#).

Image 2

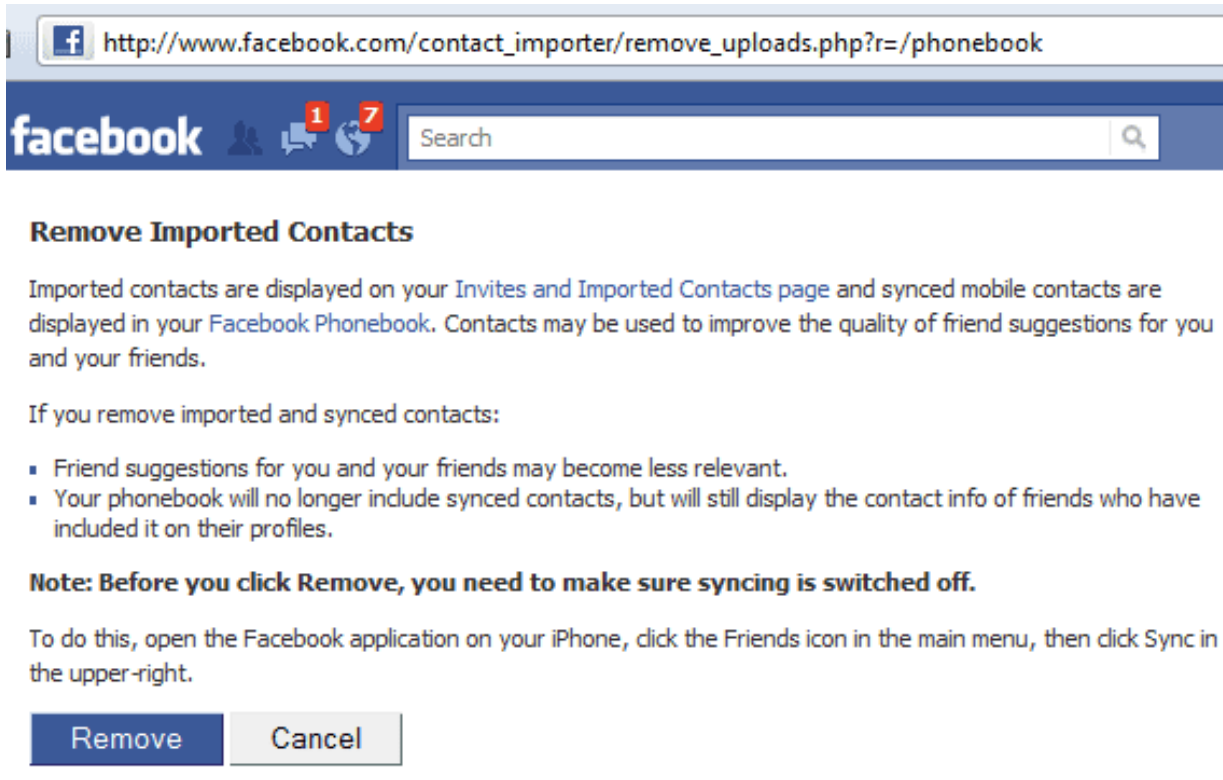


Image 3



About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the [ESET Threat Center](#) to view the latest:

- [ESET White Papers](#)
- [ESET Blog](#)
- [ESET Podcasts](#)
- [Independent Benchmark Test Results](#)
- [Anti-Malware Testing and Evaluation](#)