Search term monitoring

A new arrow for your security bow!

GFI WebMonitor™

Web security, monitoring and Internet access control

Some businesses believe that if they have anti-malware, antivirus and some firewalls, then they are safe and secure. But the world has evolved, and this is no longer the case. These precautions are no longer enough.

As BYOD and cloud thinking pervades businesses of all sizes, the nature of many hacking activists has changed: instead of finding a way to penetrate your company from outside, they build a trap outside your company security walls, and wait for your employees to wander outside your firewalls and fall into their clutches.

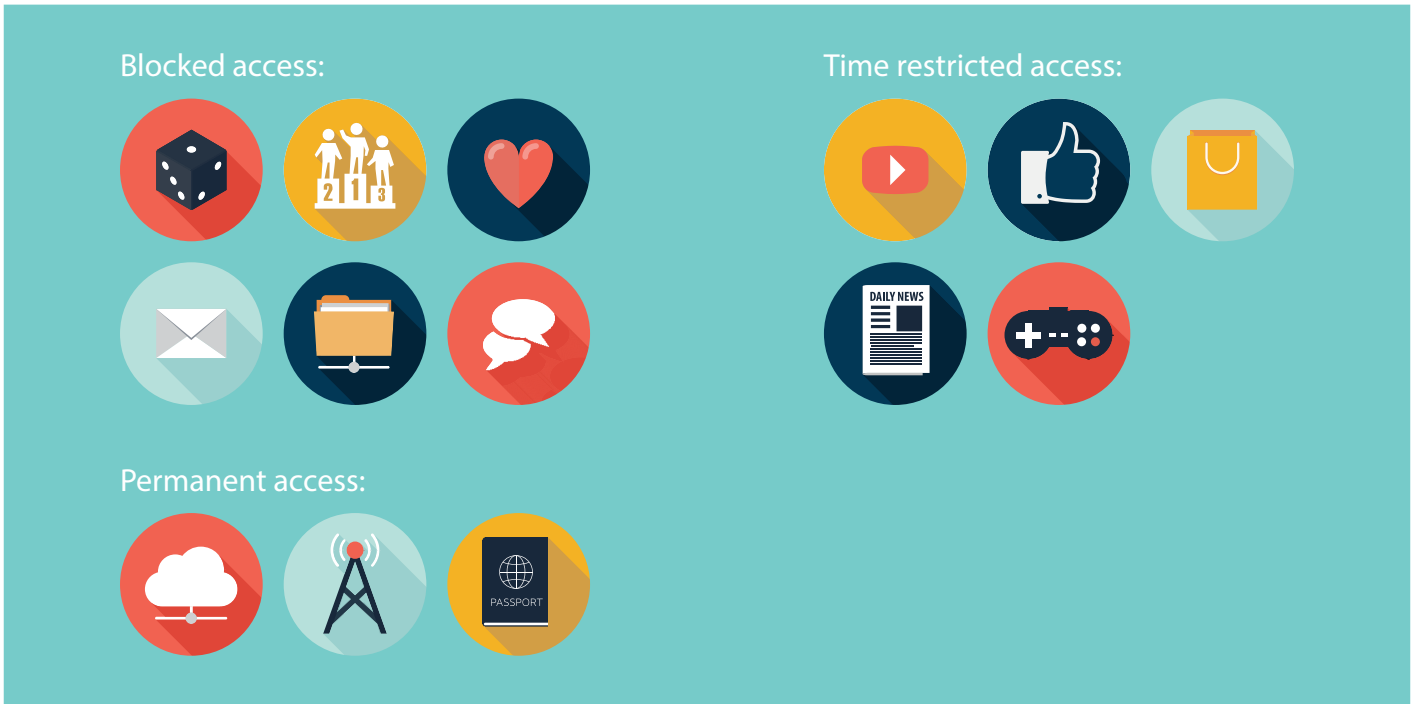
By infecting websites that users frequently visit, it is possible for a user to be lured to a 'trusted' – but comprised website, and infected with designer malware within seconds of the visit: the so-called 'drive-by-infection'.

Businesses who are aware of this risk, may have already implemented a web security and filtering solution that identifies pernicious sites and blocks them. But, by only looking at the URLs that users click on, companies are missing a security trick, that if implemented, could pay dividends: why not monitor and filter the actual terms used in the websearches conducted by the users before they click on the URL linking to an infected website?

In fact, 90% of all today's malware attacks are based on malicious URLs, most of which are clicked on based on search results.

Most companies will have an internet policy in place that dictates how their employees can use company assets to utilize the benefits of the internet, outlining what they can and cannot do when visiting the internet, and what type of sites they can visit. This corporate 'acceptable use policy' is worthless without the means to enforce it.

Search engine monitoring is one way to help stop this, and is similar to URL filtering – bad URLs or search terms can both wreak a lot of havoc. In fact, 90% of all today's malware attacks are based on malicious URLs, most of which are clicked on based on search results.



Add search monitoring to URL filtering

Search Term Monitoring is a perfect complement to URL filtering by filling in the gaps URL protection leaves behind. URLs don't always tell you what the underlying content is about, so it isn't a great intelligence tool. Search terms are the opposite, as they indicate exactly what the end user is after.

And only with search engine monitoring can you know these undesired searches are being made in the first place, and then give you the ability to control them.

Are employees searching for 'Dropbox', indicating their possible intention to use this service to work around corporate storage policies and open you up to the risk of data leakage? The same goes for Instant Messaging (IM) which may be covered under corporate policies that dictate one standard IM tool.

Some searches seem innocent but can be incredibly damaging. Do you really want your best employees looking for new jobs on company time? This can be spotted and stopped by monitoring for the words "Monster", "jobs", "Yahoo! Jobs", "careers", "resume", or the career sections of your competitors' websites.

Do you really want your best employees looking for new jobs on company time?

Admittedly, employees searching competitor's websites may be a necessary, innocent activity: after all, if you have a competitive or market analyst in your team, you want that person looking for information about the competition, and seeing what they are doing. But what about the rank and file? Are they looking for competitive insight, or searching for a hiring manager or perhaps an executive they can sell your company's confidential data to? This may sound extreme, but sadly it does happen. And if it does happen, it would be good to know.

Instead of just adding the competitor's name, add "career", "jobs" and other terms to the competitor's name to see what the end user is really after. At the same time, search monitoring also helps you understand what your end users are thinking, how they work, what their interests are, and how productive they might be.

Misdirected searches

Almost everyone has heard the old story of whitehouse.com, where this seemingly innocent URL brought users to a porn site. The site, founded in 1997, has since been taken down but not before thousands of school kids went there by accident and got an eyeful. The same happens with search terms, where all kinds of crazy and dangerous links can pop up, including an array of phishing sites.

In fact hackers, looking for the broadest base of victims possible, use popular keywords to lure users to their nefarious websites and then steal their data, money, or infect them with malware. These terms can be based on celebrities or current events. Once you key in the words you may see some legitimate appearing websites that users don't hesitate to click on.

Maybe they want you to download a video, click to enlarge an image, or worse yet, give out your credit card number to buy a non-existent product. In any case, as soon as you click on the link you are immediately and automatically compromised.

And what if a phishing attack steals your customers', rather than just your data, such as client's credit card numbers? How do you rectify that problem, and can you ever fully repair your reputation?

Security is one of the top reasons to monitor and filter search terms, but it is far from the only one.

SEO poisoning is a popular hacker misdirection trick. These hackers inject often used queries into search results using an array of techniques, sometimes with fairly simple and commonly available attack scripts. These terms then become part of Google's search cache and so appear again and again.

Hackers can also work the Google algorithms to make their bogus sites sit high in the rankings, making them seem all the more legitimate.

Another trick that works especially well on the young and the young at heart is to offer the download of a game or app. Now the executable is on the end user's computer and can have its way with the machine.

Getting something for nothing is a big hacker gambit, which is why "free music download" has traditionally been such a dangerous search phrase. In fact the chances of getting a bogus and dangerous site with that search phrase is reportedly about one in five.

Reasons to monitor search

Security is one of the top reasons to monitor and filter search terms, but it is far from the only one. Here are some others:

Know what's going on

Web searches are a window into the soul, or at least the mind. Tracking web search terms allows management to understand the interests and thinking of their staff.

On the plus side, you may be able to respond to these interests. Say there are a lot of fantasy football queries - you could form a morale-boosting football club.

It can also alert you to issues:

If there are a lot of queries about sexual harassment, it may be from a victim of harassment within the workplace, and it is then the company's responsibility to handle it appropriately.

The best way to respond to threats is to know about them.

Give insight into the 'mood' of employees

Searches can also give a general sense of the mood of your workers, something vital to creating a positive work environment. It can help HR respond proactively to employee feelings, creating initiatives to mitigate employee concerns before they become more serious. For example, if several employees are observed to start searching for information on employee rights or unions, you may realize that discontentment is growing.

Alternatively, if, for example users start searching for 'takeover' & 'a competitor name', it may be time to make an announcement to your staff to either accept, deny or 'qualify' rumours that may be circulating about a potential company merger or sale, thus addressing their concerns and providing reassurance. Uncertainty breeds discontentment, and discontentment is a known security risk: employees who begin to seek alternative employment, may start to download useful company information to private emails, or USB sticks.

If search term monitoring alerts you to this risk, it may also be time to start auditing your other security capabilities: do you have End Point Security measures in place? Have you blocked access to private emails? Do you have log management capability that may enable you to track the behavior of suspect individuals: what did they do, who did they communicate with, what information did they access, and where did they send it to, or what did they do with it?

Web problem areas

There are a number of potential web problems and to what extent they are concerns depends on the culture and values of the company you work for.

Time wasters

Some businesses want to restrict or at least know about activity relating to what they consider to be time wasting sites, such as ESPN.com. This is really a value judgment. Fortunately some tools let you limit, rather than completely block access to sports sites. For instance, you can set time limits so sports searching can be squeezed into break times, or set a browsing limit per day e.g. not more than 30 minutes a day of leisure browsing.

Humor

This is another judgment call, but some humor sites can slip in some pretty inappropriate content, at least for the work environment. And these sites often include bandwidth clogging videos. Meanwhile, searching for celebrity humor can bring your end users in direct contact with an SEO poisoning attack.

Shopping

There are two categories of shopping: consumer and B2B e-commerce. It is the first you should perhaps be worried about, mostly because of the time it can consume. But busy workers sometimes need to buy online as they don't always have time to do it physically. Here you may want to combine time limits with the blocking of sites thought to host phishing attacks.

Downloadable games are often Trojans in disguise.

Games

Another frequent target of SEO poisoning, downloadable games are often Trojans in disguise. These are a prime target for monitoring and blocking – unless you are a game company yourself doing research! In any case, at least make sure your web protection software scans all web downloads for malware.

BitTorrent and other downloaders

Download sites should be carefully restricted as they are full of pirated software and bootlegged media, - a myriad of bandwidth intensive files.

Monitoring made easy

The last thing you want are IT or management staffers spending all day watching employee search terms pop up on some management screen. You want something easy to install, administer, and which can easily help you learn about and then control undesired searches.

Even better if the Search Term Monitoring is integrated with other web protection tools, with it all being manageable through the same console. The tool should show the search terms and phrases in real time, as well as collecting them for review

later. And this historical data is great for forensics in the event of a successful SEO poisoning or other web attack.

By combining search term monitoring with web monitoring, you can gain deeper understanding of what the search was about. Say the search was about careers. But instead of looking for a new job the employee was looking for career development or training for workers. Or they were a hiring manager doing competitive analysis. Not exactly a bad thing.

Plus combining search and web monitoring gives you deeper insight into employee behavior, both individual and in aggregate.

Integration makes all the difference

Web security, search monitoring and URL filtering are essential aspects of proper security. Buying these from three different vendors makes things at least three times as complicated. First, there are three licensing or subscription plans to deal with. Secondly, there are three sources of support and upgrades. And finally, there are three very different ways to manage these tools. A unified offering makes everything easier, especially as all these elements are related and really should be intertwined.

Teach them how to spot a bogus web site.

Alerts

The best way to respond to threats is to know about them. The best tools alert either IT administrators or service providers when there are issues. Alerts can be the basis of action. With real-time access to the monitoring tool, a web connection can be terminated if the searches are deemed dangerous or the resulting actions carried out by the user following a search take up too much bandwidth, as with streaming media or video.

And if searches are attempted which seek to bypass your proxy, an alert can be sent so you can stop the search and let the user know it violates the acceptable user policy, as well as the IT policy.

Policy in place

Before beginning any monitoring program, make sure you have a security policy in place that is simple, clear and understood by employees. If possible, hold training sessions on the policy, and have employees read and sign the policy. For search term monitoring, employees should know why it is happening, how the monitoring takes place, and how they should comply with acceptable use. The policy itself, along with the knowledge that such monitoring is possible, solves at least half the problem as it instantly changes employee behavior. It's called being proactive. The other part of being proactive is the actual filtering and blocking and tracking of undesired content.

Training tips

Just as the policy is important to safe Web searching, so too is having end users understand the issues and conduct themselves properly.

Here are a few tips:

- Help your employees understand that obviously inappropriate terms are off limits
- Have them also understand the danger of common and popular search terms
- Teach them how to spot a bogus website
- Make sure they only click links they know are safe
- Make sure users don't alter security settings or mess with installed security software, agents or services

In summary, search term monitoring is a technology which, although often overlooked, provides an essential security function with today's business environment.

Furthermore, the security of any business is signicantly increased when Search Term Monitoring is combined with web security and URL filtering, ideally all on the same platform: a single platform that provides comprehensive, automatic web security management.

Such as can be found in GFI WebMonitor. For further information or to arrange a free trial please go to http://gfi.com/webmonitor.

About GFI®

GFI Software™ develops quality IT solutions for small to mid-sized businesses with generally up to 1,000 users. GFI® offers two main technology solutions: GFI MAX™, which enables managed service providers (MSPs) to deliver superior services to their customers; and GFI Cloud™, which empowers companies with their own internal IT teams to manage and maintain their networks via the cloud. Serving an expanding customer base of more than 200,000 companies, GFI's product line also includes collaboration, network security, anti-spam, patch management, faxing, mail archiving and web monitoring. GFI is a channel-focused company with thousands of partners throughout the world. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

More information about GFI can be found at http://www.gfi.com.

GFI 8070 dec13

GFI®

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us

Other network security solutions from GFI

GFI EndPointSecurity™
Control of USB sticks, iPods and other endpoint devices

GFI EventsManager™
Log data analysis and IT management

GFI LanGuard™
Network security scanner and patch management