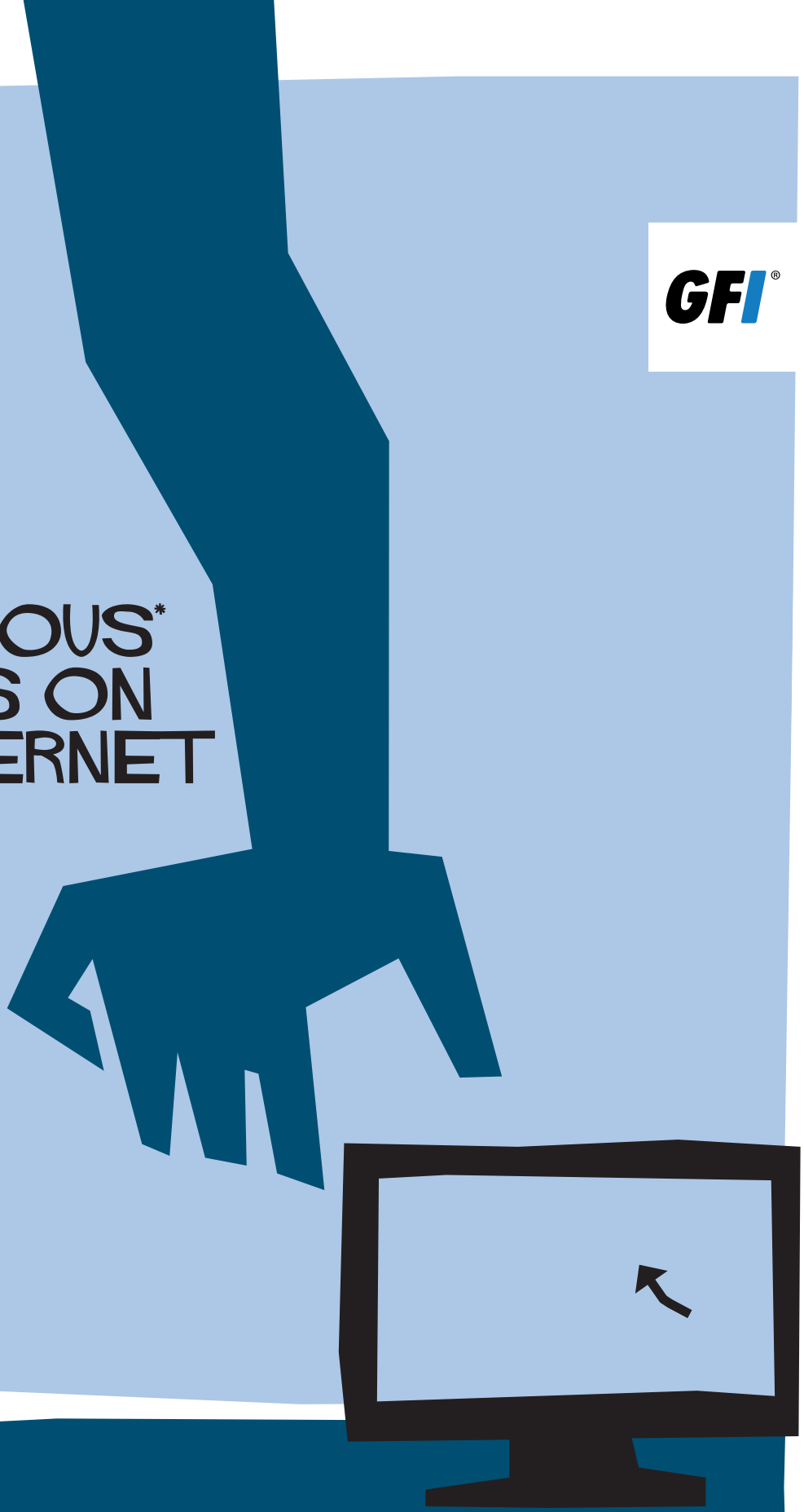
GFI®

THE MOST DANGEROUS* SITES ON THE INTERNET



*AT LEAST AS FAR AS YOUR BANDWIDTH BILL, HR AND PRODUCTIVITY ARE CONCERNED

INTRODUCTION

The movie opens with eerie music playing in the background; maybe a Theremin or a harpsichord – just not a harmonica. A desk fades into view. Too many coffee cups and fast food wrappers litter the desk. Piles of papers with headings like CCB (Change Control Board) and TPS Reports are visible. A man sits at his computer, sound asleep with his head on the keyboard, glasses askew. The screensaver blanks to a blinking cursor. Text starts to appear on the screen. Is it safe? Is it?

After a few seconds, a web browser appears on screen. A hand reaches out from the screen and starts to inch towards the sleeping man, oblivious to the terror he's about to experience. The hand moves slowly past the sleeping man, reaches into a pile of papers on the desk. Music begins to swell towards a crescendo. The hand… turns a piece of paper over, and we see…

A HUGE BILL FROM THE ISP!

The music crashes in a minor chord. Man awakens screaming, fade to black. While this might sound like the latest SyFy Saturday Night made for TV movie, or a script even Roger Corman would reject, this scene actually plays out in businesses all around the world every day. Why? Because it's not safe. We're talking about the Internet and your employees' access to it.

There are millions of sites on the web that present dangers to your users, whether it's through malware or time sinks. Countless numbers of sites exist seemingly with the sole intent of creating an HR, IT, legal or whatever other nightmare for you. And infinite are the music and video sites that offer streaming of content for free… that is, until you get the bill from your ISP for all the bandwidth your users consumed.

We've scoured the web to find a Rogues' Gallery of the most dangerous sites on the Internet. We will look at why they're great, who the big hitters are, why they can be so dangerous and what you can do to avoid your own personal horror story.

10 ONLINE HUMOR

AN ENDLESS LIST HIGHLIGHTED BY SITES LIKE 9GAG, REDDIT, CRACKED.COM

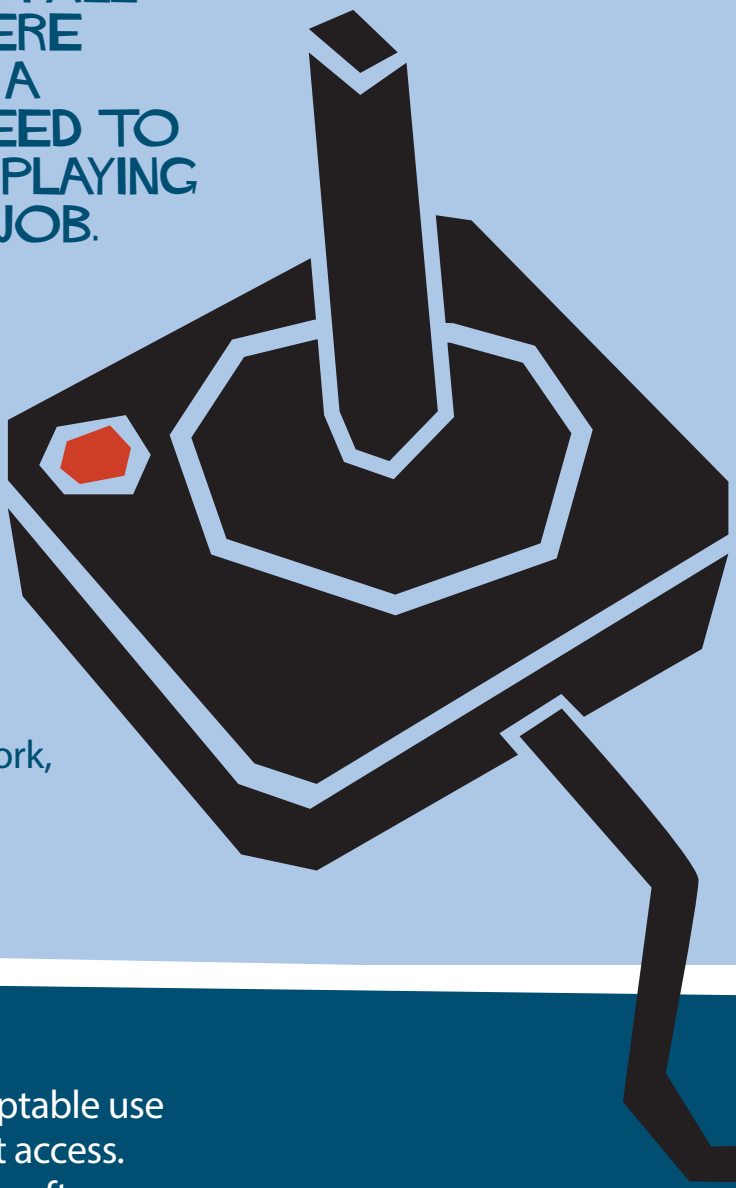
The Pros:
Access to humor on demand, whenever and wherever you are, can brighten the day and provide a much needed mini-break to help relieve the stress and refocus attention. Laughter really is the best medicine.

The Cons:
As with all sites, excessive use of humor sites can lead to productivity loss. Inappropriate content forwarded to colleagues in the office can lead to legal liability, put a burden on the email server and sometimes contain malware.

How to mitigate:
Monitor and/or limit the amount of time users can access recreational websites. Use web content filtering to block access to compromised sites or malware and ensure your acceptable use policy covers what is and is not appropriate to help users avoid potential liabilities.

9 GAMING SITES

ONLINE GAME SITES, MMORPGS AND DOWNLOADABLE GAMES FROM ALL OVER THE WEB FALL INTO THIS CATEGORY. THERE IS NOTHING WRONG WITH A LITTLE FUN, BUT USERS NEED TO UNDERSTAND THAT GAME PLAYING IS NOT A PART OF THEIR JOB.



The Pros:
A quick game to break up the day during a scheduled break or at lunch should be okay with most, and can help lighten moods, refocus attention, and generally make people smile.

The Cons:
Quick games can easily waste hours at work, and some downloadable games may be Trojans carrying malware.

How to mitigate:
Define what is and isn't okay in your acceptable use policy. Use bandwidth restrictions to limit access. Scan all downloads with Internet filtering software to reduce the risk from malware.

8 ADULT CONTENT SITES

WHAT CONSENTING ADULTS CHOOSE TO DO AND/OR VIEW AT HOME IS THEIR BUSINESS, BUT IN THE OFFICE THERE ARE CERTAIN THINGS THAT JUST ARE NOT APPROPRIATE.

I bet you expected a list of sites for this category, didn't you?

The Pros:
There really aren't any when it comes to viewing mature content at work.

The Cons:
Offended employees filing complaints with HR or lawsuits in court, malware infecting machines, loss of productivity, damage to morale, and those awkward and embarrassing moments where you realize you know more about the person you are working with than you ever really wanted to.

How to mitigate:
Web content filtering that blocks access to mature content combined with an acceptable use policy that everyone can understand.

7 ONLINE SHOPPING

The most popular:
eBay and Amazon

The Pros:
If you're looking for a bargain or the latest novel to hit the bookshelves, eBay and Amazon respectively are fantastic tools. Log in, find what you want, and pay. Simple, fast and users don't have to go to the store!

The Cons:
Productivity loss can be a significant factor with users spending more time browsing for stuff that they DON'T need to know about during office hours.

How to mitigate:
Monitor users' Internet access. Use an acceptable use policy to make clear the company's expectations.

The most dangerous:
Craig's List, others

The Pros:
Localized shopping for anything from cats to cars makes it easy for users to find what they need.

The Cons:
Craig's List posts may be phishing attempts in disguise or verge on the illegal, while other online shopping venues may be completely fraudulent.

How to mitigate:
Combine user awareness with web content filtering that blocks access to known phishing sites.

6 CLOUD STORAGE

DROPBOX, GOOGLE DRIVE, BOX.NET, MEGA, SKYDRIVE AND OTHERS OFFER USERS HUGE ONLINE STORAGE REPOSITORIES, WITH LITTLE TO NO CONTROL OVER WHAT USERS STORE OR SHARE WITH OTHERS.

The Pros:
These services can alleviate local storage related problems, enable easy sharing of large files, and provide users with an online backup of their data.

The Cons:
These services can also introduce privacy issues, create a huge bandwidth drain and become a legal liability, especially when customer or NPI data is stored, or the sites are used for access to and sharing of copyrighted material.

How to mitigate:
Enforce bandwidth limits. Use web filtering to block access to these services for users who do not need this access to prevent downloads of illegal material.

Create a policy that requires users to only store company content on company-controlled resources. Many of these services offer a business version as well as a personal one.

5 INSTANT MESSAGING

SITES AND SERVICES LIKE SKYPE, CHAT ROULETTE AND EBUDDY

The Pros:
Skype and other IM (Instant Messaging) sites are fast and simple communication tools that can be used as an alternative to email – which can take a while; and to calls which can be disruptive. You can even set up video calls with your colleagues from worldwide offices.

The Cons:
For every legitimate use of the service, there are probably hundreds of illegitimate or inappropriate uses, including the sharing of content completely inappropriate for the workplace; also, IM sites can be used at work for personal chats or for non work-related conversations with colleagues.

How to mitigate:
The best choice here may be to block access using web content filtering, or to ensure that users understand how to use the services safely.

While being able to Skype with a customer may be good for business, random webcam chats with strangers can, if you'll pardon the pun, expose users to much more than they bargained for.

4 DOWNLOAD SITES

ACCESSING CONTENT FROM P2P, TORRENTS AND WAREZ SITES

The Pros:
Downloading ISOs of open source operating systems and applications can help get good content distributed quickly and cheaply.

The Cons:
There's a lot more copyrighted or compromised content that can lead to legal liability or infect machines with malware.

How to mitigate:
Once again, a web content filtering solution supporting a good acceptable use policy is the right strategy to take.

3 SEARCH ENGINES

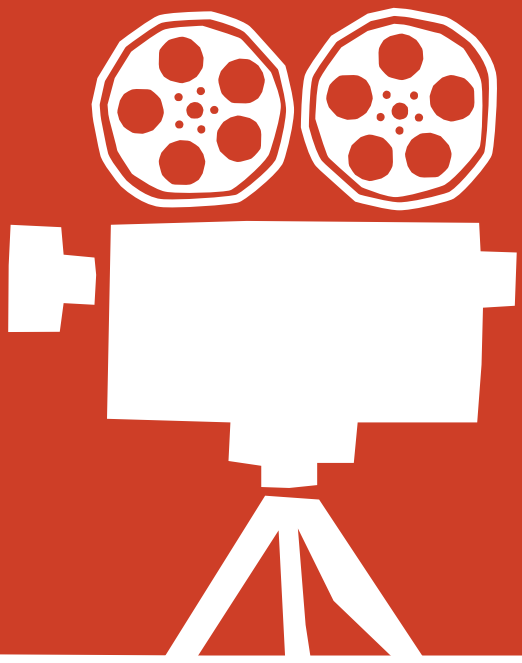
THE MOST POPULAR: GOOGLE, YAHOO! AND BING

The Pros:
Search engines connect users to a massive source of information, that is, the Web. Within seconds, users can find whatever they want on any subject – all they have to do is type in the relevant keywords.

The Cons:
Search engines can provide access (accidental or intentional) to content inappropriate for work. SEO poisoning can lead users to access compromised websites.

How to mitigate:
Protect users by enforcing safe-mode browsing. Use web content filtering to scan all downloads for malware.

2 STREAMING MEDIA



The best:
YouTube

The Pros:
YouTube contains videos that enable users to do research, learn about technology and best practices, increase awareness, and view additional content not available on TV.

The Cons:
YouTube viewing can be bandwidth-heavy especially in organizations with limited bandwidth streams. It also contains tons of entertainment content that is not even remotely related to most companies' business interests.

How to mitigate:
Monitor bandwidth usage, enable web filtering and ensure your acceptable use policy defines what is and isn't acceptable.

The rest:
Spotify, Soundcloud and iTunes

The Pros:
Enables users to access their media such as music and video while reducing storage needs.

The Cons:
Consumes huge amounts of data rendering access to other Internet services much slower.

How to mitigate:
Monitor and limit bandwidth usage as necessary to strike the right balance between access to services and other bandwidth requirements.

1 SOCIAL MEDIA

The most notorious:
Facebook

The Pros:
It's a great marketing tool, a way to keep in touch with your customers, to do research on the competition, among other things.

The Cons:
It can contain spam, malicious links, apps that could cause a decrease in productivity, can be used as social engineering tool, and can cause apparent tears in the space-time continuum. Users might intend to just make a quick "check in" or status update only to find an hour later they completely missed a meeting.

The coolest:
Twitter

The Pros:
It's another great marketing tool, a way to keep in touch with your customers in real-time and a very personal way, can serve as an instant news feed, and to take the pulse of a community. Many management and monitoring tools use Twitter to provide alerts, and more service providers use it to push updates to their users.

The Cons:
Hijacked accounts are used to send malicious or spam content, can be misused as a vector for information leakage or PR fiascos, and can also be a time sink.

How to mitigate:
Ensure user web browsing is monitored and protected, and limit the amount of time (or set specific times) that sites like this can be accessed. Make sure your Acceptable Use Policy addresses what is and is not acceptable when it comes to social media sites.

The others:
Tumblr, WordPress and the millions of other blog sites out there

The Pros:
There's some incredibly useful content on many of these sites, especially for IT admins looking for how-to and fix-it posts, or reviews of IT solutions from other IT admins.

Cons:
Like so many others, these sites can become an enormous time sink, can often contain material that is inappropriate in an office, and may host malware, either intentionally or unknown to the sites' owners.

How to mitigate:
Web content filtering combined with good antivirus software on workstations should bolster a well-written and understood acceptable use policy.

REMEMBER

The Internet is full of wonder and joy, but it is also fraught with peril and the risks to your users and your company's data, are very real. Users are adults and should be treated as such.

Your best tool is an acceptable use policy that is fair, balanced and easy to understand. But it should not be your only or even your last line of defense.

Internet filtering can help prevent accidents, stop users from breaching corporate policies, and when they lose track of time or have spent too much time streaming media, remind them that they need to get back to work.

Protect your users, your company's IT resources, and your customers from the most dangerous sites on the Internet. You don't want the SyFy Saturday Night made for a TV movie to become your reality, do you?

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