
Hacker-cracker-attacker:
see your network like the bad guys do
GFI®

They are out there

Lurking in the deep, dark corners of the web. Hiding in plain sight among the multitude of websites you would consider not only business-related, but also business critical. They masquerade as basic functionality data downloads or embedded media. They are malware, and they exist for one thing and one thing only – to do no good.

Maybe it is your users they target or perhaps your family and friends. They could be after your neighbors, or perhaps even you are in their sights, because even sysadmins have been known to click on the wrong link or visit the wrong page.

In this ebook we are going to take a look at how the hackers, crackers and attackers see your network. We will look at each of the attack vectors the bad guys can use to take advantage, or even ownership, of a remote machine. We will look at the unpatched, legacy and the misconfigured systems that live on your network every day and how they are at risk.

We will also examine the different kinds of malware that can exist within webpages. We will look at what they are, how they can get there and what they can do to their unsuspecting prey.


We will also look at what sysadmins
can do to protect users and user
machines from attack
GFI

ANATOMY OF A VICTIM

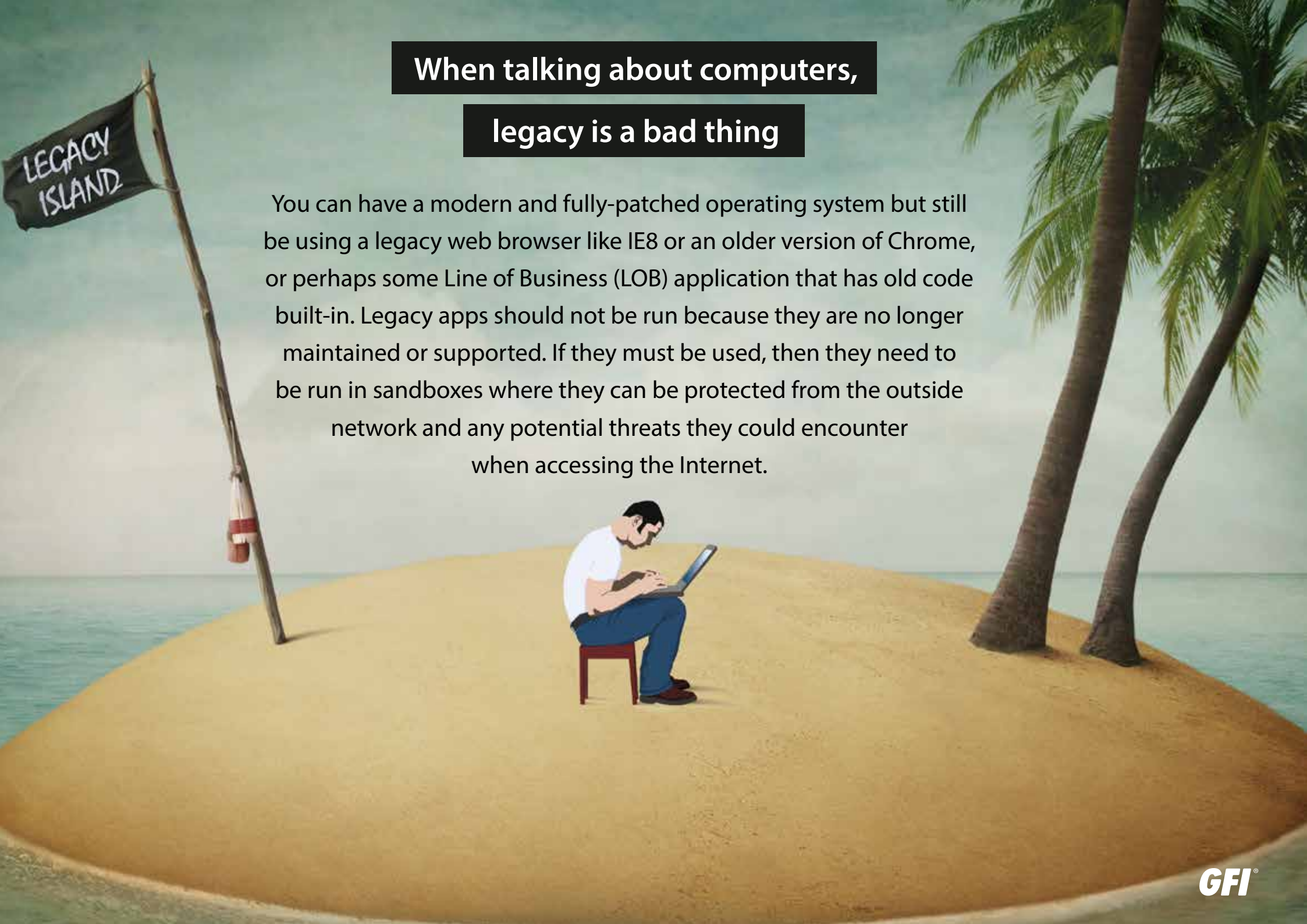
Before a user can become a victim, the attacker has to have some way to get code to them. When we're talking about Internet access this means the user must visit a website that the attacker can use to exploit their victim. While no system is 100% secure from any threat, some users just make it too easy for attackers.

GFI®

EOL means end of life – why you should care

Windows XP was awesome. So was that pizza you had for lunch last week. But all good things must come to an end and just like you throw away the leftovers, you need to let go of XP once and for all. Operating systems that reach their end-of-life no longer get patches or updates and that means that if an attacker discovers a flaw, there won't be any fix from the manufacturer. XP is not the only thing that needs to be let go. Mac OSX 10.6 and earlier versions are also EOL and that means users need to stop using them or they could become a victim.

GFI®



When talking about computers, legacy is a bad thing

You can have a modern and fully-patched operating system but still be using a legacy web browser like IE8 or an older version of Chrome, or perhaps some Line of Business (LOB) application that has old code built-in. Legacy apps should not be run because they are no longer maintained or supported. If they must be used, then they need to be run in sandboxes where they can be protected from the outside network and any potential threats they could encounter when accessing the Internet.

GFI®

PATCHES?

WE DON'T NEED

NO STINKIN'

PATCHES!

If you have gone more than a week without patching something, then you know, as a sysadmin, that something is wrong. Some companies only patch once a quarter and some users don't patch at all. New vulnerabilities in operating systems and applications are discovered every day and the best and only way to mitigate the threats is to patch. Frankly, if you're not patching and you use an unpatched machine to access the Internet, you are asking for trouble.

GFI®

Like shooting fish in a barrel

No matter how many times we are told not to, we all probably launch a browser or check our email using an account that has 'admin rights'. Many of us probably deal with users who have admin rights on their own machines. It's no wonder malware payloads can execute with admin rights when the browser is running in the context of an administrator, and antivirus software can be turned off because 'it slows things down!' If you are surfing as an admin, you're probably too much of risk-taker.

Types of malware

Malware comes in all sorts of shapes and sizes and different attacks have different vectors and surfaces. Whether an attacker just wants to cause damage, to steal credentials, to get valuable data, find a back door into your system, or 'use you' to make an even bigger score, they must first get you (or your machine) to do something bad, like run code. Here are the biggest offenders in the malware realm.

GFI®

Malicious scripts

Javascript can be contained within a webpage and when you combine malicious code, vulnerable browsers, admin rights and no anti-malware software, you have the perfect storm that permits an attacker to compromise a machine. All a user has to do is visit a page. Gone are the days when you had to have some kind of scripting engine and actually download and run code… you execute Javascript nearly every time you visit a website.

Infected files

Sometimes the oldies are still the goodies and infected files that users download and run are still a sure thing for bad guys to use. Screensavers, new desktops and media codecs are just a few of the file types that attackers can post which contain malicious code. If a user downloads and runs them, they get an instant 'promotion' to victim.

Embedded media

As long as webmasters embed media files and users click on them then infected media embedded in webpages will be used to great effect. Media players need updating almost as often as operating systems. Unfortunately without patch management, enterprises have an impossible task to complete if they want to make sure their users' machines are kept up-to-date.

Attack vectors

A dynamic website is a fun but dangerous place to visit. Dynamic content is the name of the game and everyone wants a piece of the advertising revenue. Since advertisers cannot count on users to click an ad anymore, they get impressions by automatically launching audio and video or putting ads in front of the content users actually want to see.

And then there is the alarming trend of putting all real content into PDF, so you have to download a file rather than just viewing data in your browser.

Here's how dynamic websites can create your worst security nightmares.

Owned websites

While not always necessary, some attackers either use their own websites to attack users or completely take over a legitimate website to do the same thing. In the former, they must somehow get users to visit the site, but in the latter, users are probably already doing that through their homepage, favorites and bookmarks.

Spoofed domains

Domain spoofing, whether by compromising DNS or taking advantage of typographical errors, is a very effective way to exploit victims. It only takes one wrong letter wrong to turn a fun website into a bad trip. If your users don't realize that they are not visiting a trusted site they might do really bad things before they realize it.

Phishing attacks

Phishing attacks are one of the most effective ways to deploy malware, but at the same time one of the most easily preventable – if only users would pay attention. Phishing attacks are so pervasive because they are so successful. At their most simple, phishing attacks that deploy malware consist of 'click here' to do something that seems like you should or even want to do it.

Cross-site scripting

Cross-site scripting attacks enable attackers to inject client-side scripts into vulnerable web pages which when viewed by other users, leads to their browser executing the script. They can be used to steal credentials or download and install malware.

Malicious links

Hyperlinks exist to be clicked and far too many users (and admins) will click on anything in an email, on a webpage or in a forum post. Attackers don't have to do anything but put a link into a discussion thread and wait… someone will click on it. Sometimes it may be as harmless as a rick-roll, but other times it can go to a webpage hosting malicious code.


DAMAGE DONE
ONCE AN ATTACKER GETS A USER TO WHERE THEY SHOULD NOT BE, ATTACK CODE EXECUTES. WHAT'S THE WORST THAT CAN HAPPEN, YOU ASK? A LOT.
GFI

Viruses

A machine infected by a virus, or many viruses, may never be considered trustworthy again. For many sysadmins, the only choice is to dust off and nuke it from high orbit; which is to say format and reimage. Hopefully you have a trustworthy backup of the critical data and a spare machine so the user isn't down for hours.

Deleted files

Some malware goes for the punch below the belt, deleting critical data from workstations, removable drives and network shares. Without good backups, this can be devastating to victims, especially when it is something irreplaceable like family photos or key customer quotes.

Encrypted files

One of the latest threats to users is ransomware. Victims' files are encrypted and they can get the key to decrypt the files as long as they are willing to pay up. No payment, no more data. It's digital extortion.

Zombie plagues

Other malware can turn victims' machines into zombies, ready to participate in attacks against other victims. Zombies can launch massive denial of service attacks, spew out spam or be used to help break into other systems through brute force or distributed cracking.

RATs

Remote Access Trojans leave back doors in computers, allowing an attacker to remotely access the server at a later time. RATs can be used by attackers to steal data or even to spy on victims through their own webcams and microphones.

What can we do now?

With so much stuff out there that targets us and our users what can sysadmins do?

Actually quite a bit.

GFI®

Patch operating systems

Patch, patch, patch. One of the most important and critical things you can do is patch. Patch operating systems, patch applications, patch the network infrastructure and keep patching because that's a task that will never end. Since it will never end, get a patch management application to help you with that. That will pay for itself in no time at all, considering it will patch third-party apps like media players!

Upgrade browsers

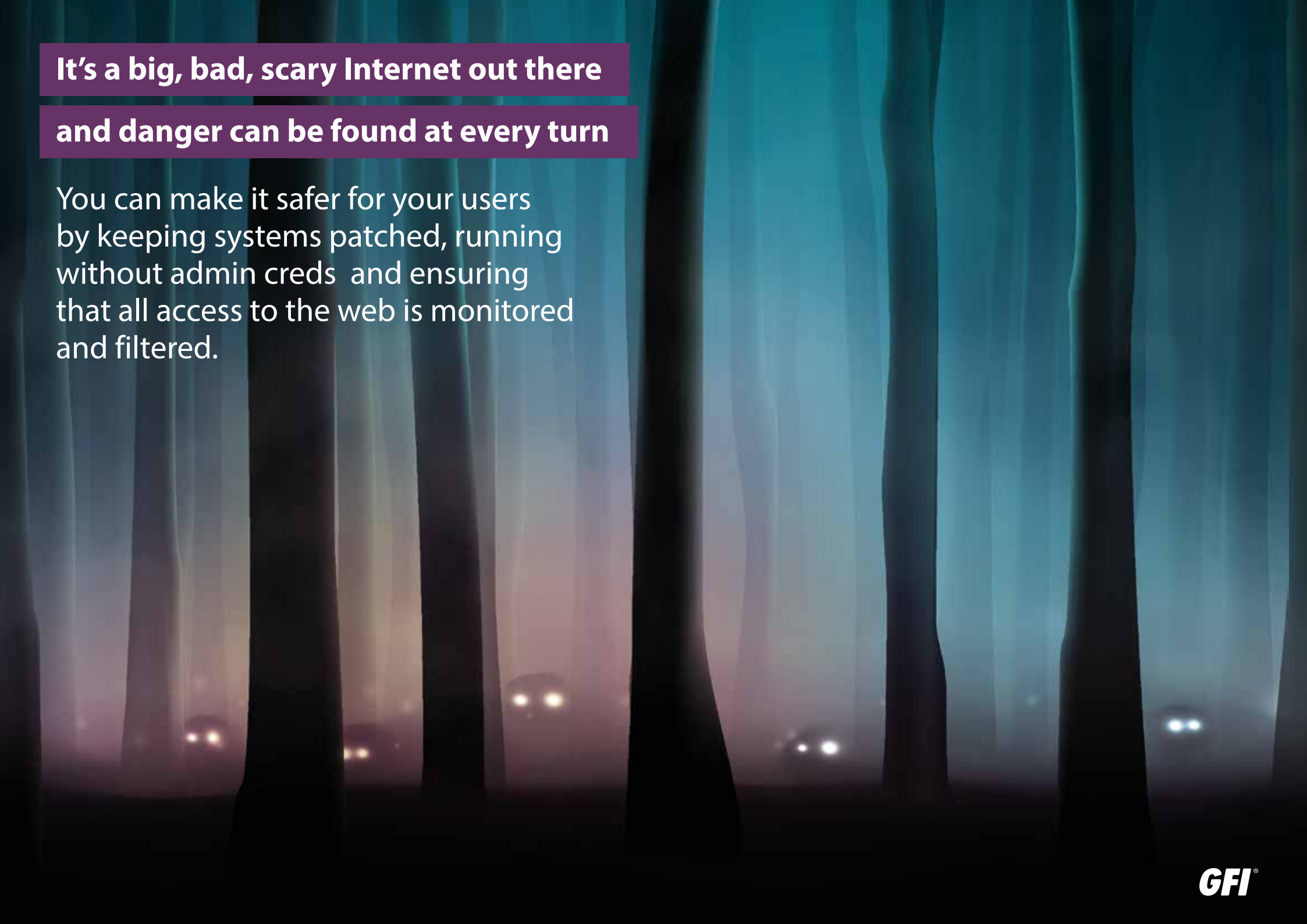
No users should use older browsers. The threat from Internet-borne attacks is so significant that if you have a legacy app that requires you to use an out-of-date browser and you cannot lose the app, you should virtualize browsers that can only be used for the legacy app and let your users run modern browsers to access the Internet.

Filter email

Ensure that you have message filtering in place to block phishing messages and to trap bad links in messages before they get to users' inboxes. So many attacks originate in users' email that you have to filter incoming messages or run the risk that users will fall victim again and again.

Monitor your downloads

The most important and effective thing you can do to protect your users from hackers, crackers and attackers on the web is to monitor your users' web activity and downloads. Use web monitoring and filtering software to protect your users from all manner of threats. Web monitoring can block users from accessing phishing, hacked and inappropriate sites. Web filtering can look at all the HTML and Javascript that makes up webpages, examine every embedded document and media file and screen all the file downloads to ensure that there's no malware present in anything your users might access from the Internet. That way, no matter what vector might be used, or which type of malware an attacker wants to deliver to your users, they are protected.


It’s a big, bad, scary Internet out there
and danger can be found at every turn
You can make it safer for your users by keeping systems patched, running without admin creds and ensuring that all access to the web is monitored and filtered.
GFI®

www.gfi.com

Follow us: