Increase your Internet immunity!

Understanding today's top online threats and how to guard against them

GFI®

The Internet is both a valuable resource and a dangerous place: Its open nature provides many benefits to the well-intentioned people using it, but also serves as a breeding ground for malicious activity. You can surf the web, access email, download content, shop and bank online, and register for contests, giveaways and access. But as you do, your chances of downloading malware or giving away sensitive information continue to grow.

The idea that increased Internet usage equates to increased exposure to Internet threats makes perfect sense. Web usage continues to climb, with one-third of the world's population accessing some form of Internet content.[1] And it often comes at a price.

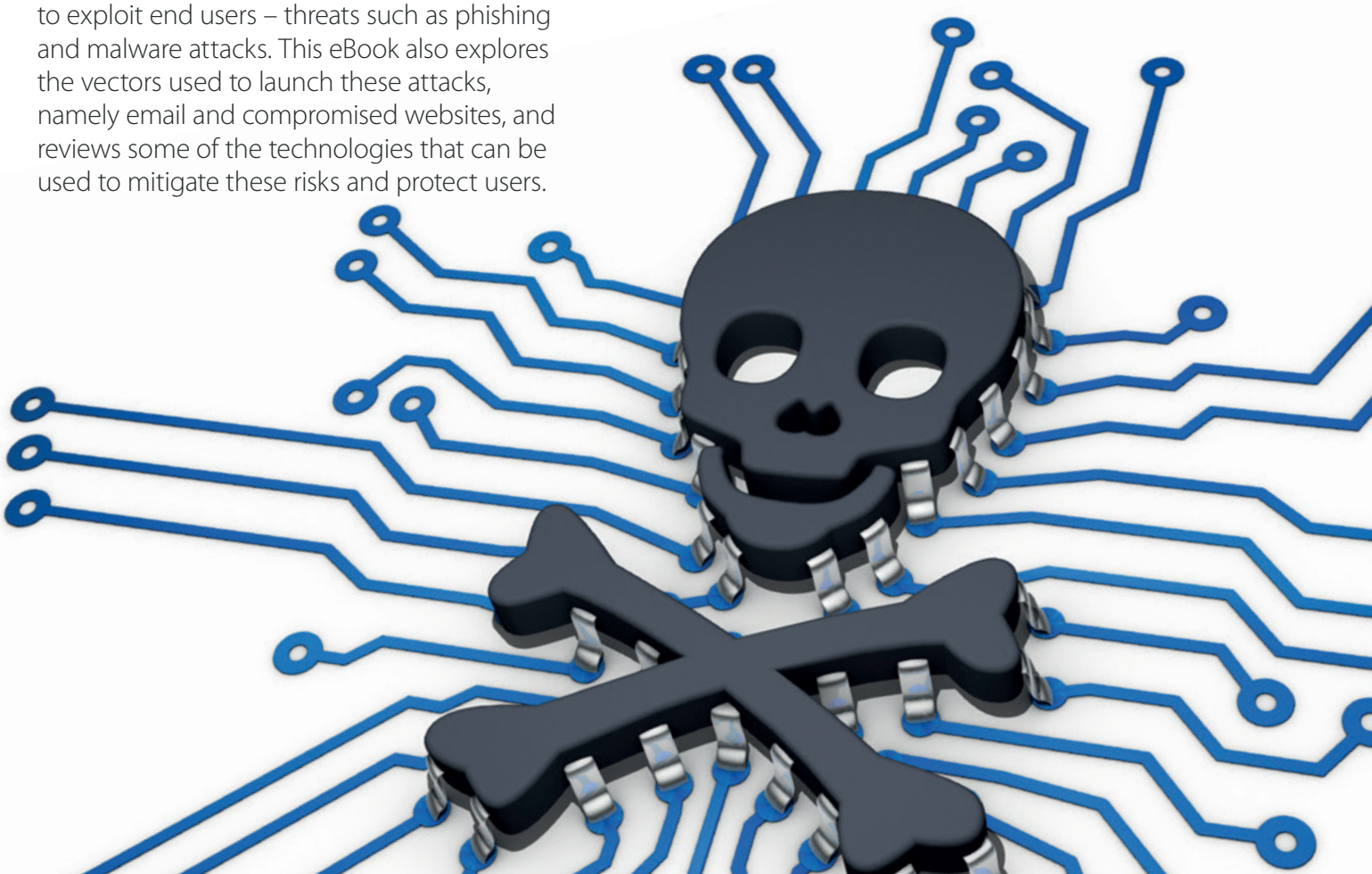
To defend against these threats, both IT administrators and end users need to understand what the threats are and how to counter them. Attackers are becoming more tech-savvy and devious at the same time. Meanwhile, awareness lags behind, increasing the likelihood that users will be exploited.

This eBook examines some of the most significant corporate network threats designed to exploit end users – threats such as phishing and malware attacks. This eBook also explores the vectors used to launch these attacks, namely email and compromised websites, and reviews some of the technologies that can be used to mitigate these risks and protect users.

Recognizing today's 'cyber-symptoms'

Phishing

Phishing attacks are targeted attacks designed to obtain sensitive and, often times, confidential information. This can include financial information, credentials or other data that an attacker, masquerading as the victim, can then use to gain unauthorized access to systems and information. According to the most recent report on phishing published by the Anti-Phishing Workgroup (APWG), "the number of phishing sites detected jumped almost 30 percent, from 38,110 in June 2013 to 49,480 in July 2013, and stayed at the higher rate throughout the third quarter."[2]



At any time, there are literally tens of thousands of online phishing sites designed to look like payment services websites, such as those used by banking and credit card companies. There are frequent imitations of corporate portals, social networking sites and other sites that end users regularly visit and enter sensitive information.

According to the same report from the APWG, payment services sites made up more than half of the most targeted industries for that same period of time.[3]

Phishing sites are hosted around the world, with the United States leading the pack, typically hosting more than half of all detected phishing sites during any particular month. The rest of the top 10 can vary greatly month to month, but all tend to be more developed countries with laws against the likes of phishing, fraud and computer fraud. It seems, however, that legislation is not sufficient; enforcement has yet to catch up to the Internet age.

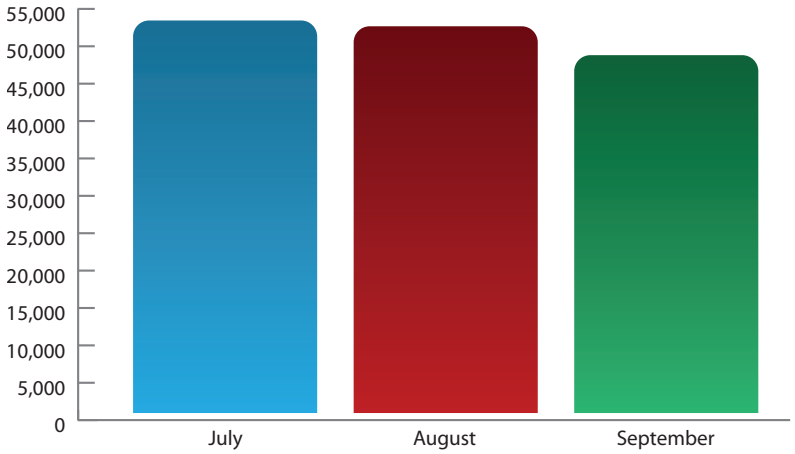


Figure 1-From the APWG's Phishing Activity Trends Report, Quarter 3, 2013

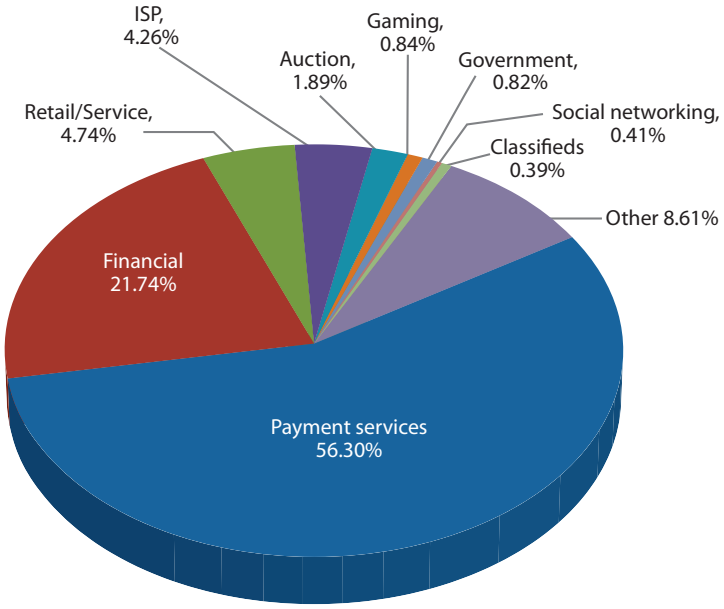


Figure 2-From the APWG's Phishing Activity Trends Report, Quarter 3, 2013

Countries hosting phishing sites - Q3 2013

July		August		September	
United States	58.78%	United States	50.60%	United States	52.58%
Canada	4.21%	France	5.85%	Germany	5.68%
Germany	3.55%	Canada	4.56%	United Kingdom	5.15%
Ukraine	3.32%	Netherlands	4.23%	France	3.35%
Russian Federation	3.05%	Germany	4.08%	Brazil	3.21%
United Kingdom	2.47%	Romania	3.83%	Russian Federation	3.03%
Brazil	2.35%	Russian Federation	3.16%	Netherlands	2.60%
Turkey	2.32%	China	2.89%	Canada	2.21%
France	2.21%	United Kingdom	2.49%	Romania	1.58%
Netherlands	2.21%	Turkey	2.47%	Turkey	1.37%

Figure 3-From the APWG's Phishing Activity Trends Report, Quarter 3, 2013

Malware

Malware continued to plague Internet users throughout 2013. It's estimated that nearly one-third of all computers worldwide were infected with some form of malware.

Malware infiltrates systems in a variety of ways.

Users can:

» Inadvertently download it directly.

» Inject it into a browser session from an infected website.

» Open infected attachments via email.

» Pass dangerous files to others with external media (e.g., USB drives).

However malware invades a computer, it can do significant damage once executed. An infection can potentially:

- Destroy data or encrypt it until a ransom is paid.
- Sit silently in the background to capture high-level credentials and other confidential information.
- Infect the computer's resources to spread spam or take part in botnets for Denial of Service (DoS) attacks.

Again, countries with a strong Internet presence, widely available commercial hosting facilities, and laws that prohibit online threats but lag behind in enforcement lead the list of places where infected websites and malicious downloads reside:

According to data compiled by APWG members, more than half of all computers in China may be infected. Russia and Canada are not far behind, with at least one-third of all computers infected. Even the UK and Australia are greatly impacted, with one-fifth and one-quarter of all computers infected, respectively.

Here's a breakdown of the top 10 countries through Q3 2013:

Ranking	Country	Infection Rate
1	China	59.36%
2	Turkey	46.58%
3	Peru	42.55%
4	Russia	41.80%
5	Taiwan	39.06%
6	Argentina	38.50%
7	Brazil	38.21%
8	Chile	36.02%
9	Poland	35.45%
10	Canada	33.83%

Figure 5-From the APWG's Phishing Activity Trends Report, Quarter 3, 2013

July		August		September	
United States	36.32%	United States	62.32%	United States	44.67%
Germany	25.12%	Germany	8.90%	Russian Federation	22.00%
Switzerland	11.92%	Russian Federation	6.46%	Germany	6.49%
Russian Federation	4.94%	Netherlands	4.50%	China	6.15%
Netherlands	3.87%	Switzerland	3.80%	Spain	4.26%
China	3.54%	China	3.04%	France	3.52%
Spain	2.23%	Spain	1.81%	Netherlands	2.18%
Korea Republic	1.84%	Ukraine	1.24%	Luxembourg	1.53%
France	1.07%	France	1.13%	Korea Republic	1.42%
Taiwan	0.85%	Korea Republic	1.02%	Ireland	0.81%

Figure 4-From APWG's Phishing Activity Trends Report, Quarter 3, 2013

Filling your 'cyber-medicine' cabinet

Since the Internet is filled with so many threats, it can be tempting to unplug users from access for their own protection. Of course, that is neither practical nor advisable, considering the Internet's positive impact outweighs the negative. The best approach is to educate users on Internet "best practices" by offering frequent training sessions. Implementing strong technical controls and defenses to protect users as well as the company is also highly recommended.

The SANS Institute offers some great resources for helping to educate your end users at the Securing The Human website. With content targeted for everyone from your end users to your developers and engineers, jumpstarting a security awareness program has never been easier. While much of their training is offered for a fee, there are resources available at no charge to help you get started with an awareness and education program.

Consider a combination of email newsletters, posters/banners and monthly brown-bag lunch sessions to continuously deliver the messages around Internet security and safety. You should make sure your users are aware of important security patches when they come out, and how to patch their own systems at home. Increase awareness of phishing schemes and what to look for in a suspicious email. Encourage the use of encryption at home and require it at the office. Ensure that no user systems run without antivirus software, and that no users at home have any excuse for failing to protect their personal computers.

The following methods provide powerful boosts to your protection plans.

Mail filtering

Email is one of the most significant vectors for infection, and can be one of the easiest for you to protect.

Think about it: Email is a central system and you control how all messages route into and out of your corporate environment. Implementing a mail filtering system is a straightforward way to help protect users from both phishing emails and malware-infected attachments. It is up to you whether you deploy a system that is installed on servers in your own datacenter, software on your email servers, or a cloud-based solution that filters out dangerous messages before they ever reach your border.

Whatever method you choose, a mail filtering system can help minimize the chances of any infected attachment reaching a user's workstation. It also helps protect your users from falling victim to a phishing scam.

Web filtering

At many companies, Internet access is a decentralized system, where the company may provide DNS services and the Internet connection, but does not use any form of proxy or filtering solution out of a sense of respect for users' privacy (or a desire not to become the "Internet police"). While providing your users with unrestricted access to the Internet is a noble and generous thought, it is far too dangerous to continue. You do not have to play chaperone or web cop to protect users from malware downloads or compromised websites.

Web filtering software can automatically scan website access and file downloads to filter out malicious scripts and block infected files before users' workstations become compromised. In the meantime, users still enjoy an open and otherwise unrestricted web experience.

Companies that want to ensure Internet usage remains reasonably business-related and do not wish to negatively impact productivity can further leverage web filtering systems. They can block access to inappropriate content, or restrict the amount of time users can spend on recreational or social media sites. All of this can be achieved while still respecting users' privacy.

Conclusion

According to research done by the Ponemon Institute, the average cost of a data breach is $188 per record.[3] Consider how many records you keep on hand for your customers, vendors, suppliers and employees.

Now multiply that number by $188 to get an idea of just how costly a security incident could become. Mitigation is a far more cost-effective strategy to follow.

The Internet remains both an invaluable resource and an incredible risk for users. It's bad enough that their home computers may become infected, but when they use those home computers to work on company files or access company resources such as webmail, the threat easily extends to their employers. Rather

than prohibiting such access, companies would do better to start with good user education. Ensure users understand the importance of:

- Keeping their home computers up to date
- Maintaining antivirus software
- Being suspicious of email attachments or links to things that sound too good to be true
- Validating any communications from banks or financial institutions, or even their own employer

Those are all defensive actions users can take. Additionally, using mail and web filtering, and strong antivirus solutions will help to establish a layered defense. Adding on best practices such as least privilege access and file encryption, along with good backups, will further strengthen the defense, and help to counter many of today's online threats.

---

[1] http://www.internetworldstats.com/stats.htm - World population of 7,017,846,922 and 2,045,518,376 estimated Internet users on June 30, 2012.
[2] http://docs.apwg.org/reports/apwg_trends_report_q3_2013.pdf
[3] https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

About GFI Software

GFI Software™ develops quality IT solutions for small to mid-sized businesses. Serving an expanding customer base of more than 200,000 companies, GFI's product line 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.

GFI WebMonitor™

GFI WebMonitor *enables organizations to monitor Internet browsing activity and block access to high-risk sites.*
Learn more at: www.gfi.com/products-and-solutions/network-security-solutions/gfi-webmonitor

GFI MailEssentials®

GFI MailEssentials *makes managing business email easy and efficient by protecting your network against email-borne junk, viruses, spyware, phishing and other malware.*
Learn more at: www.gfi.com/products-and-solutions/email-and-messaging-solutions/gfi-mailessentials

For more information about GFI's network and security solutions, visit our website: www.gfi.com

www.gfi.com

GFI Software, 4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA
Tel: +1 (888) 243-4329 | Fax: +1 (919) 379-3402 | ussales@gfi.com

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