

# 10-STEP

action plan for the

# ULTIMATE

email protection



**GFI MailEssentials®**

# Contents

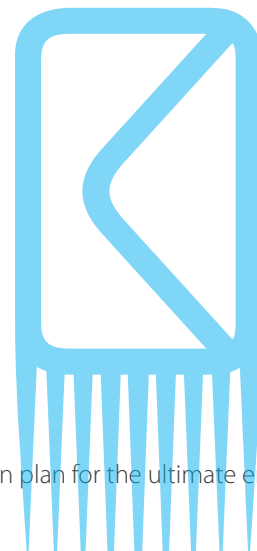
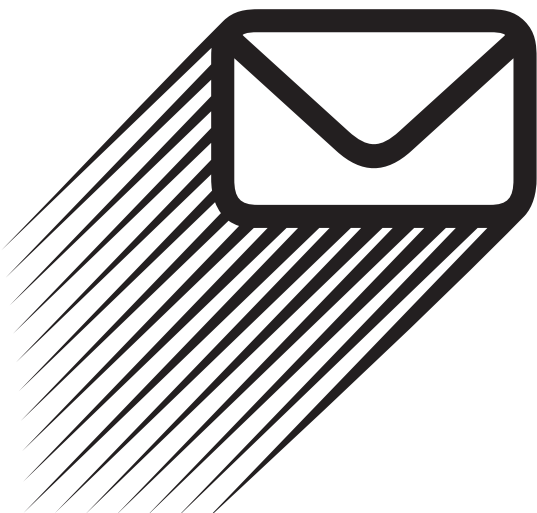
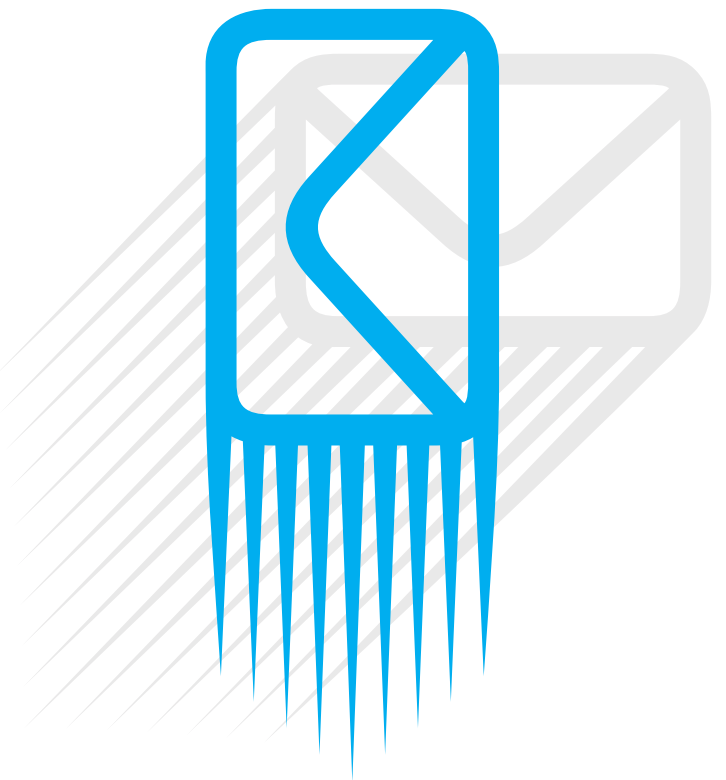
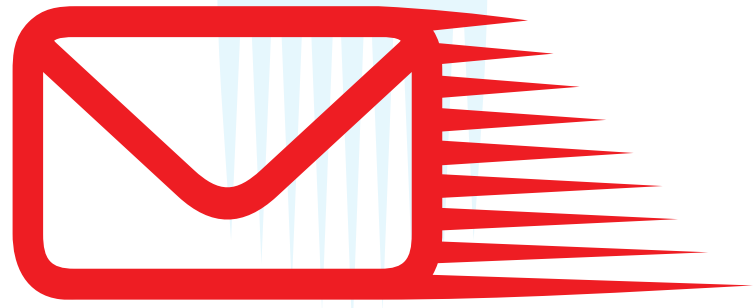
Why is email so vulnerable?.....	4
What harm can hackers do via email?.....	5
Attacks broaden and worsen.....	6
Spam still a problem, maybe more than ever.....	7
The new ThingBot threat.....	8
It's time to fight back .....	9
Step 1: Proper passwords.....	10
Step 2: Block data leakage.....	11
Step 3: Stop spam before it really stinks.....	12
Step 4: Controlling content via filtering and monitoring.....	13
Step 5: Make malware go away.....	14
Step 6: Block breaches.....	15
Step 7: Compliance.....	16
Step 8: Training and best practices.....	17
Training tips and tricks for your users.....	18
Step 9: Fight phishing.....	19
Step 10: Implement defense in depth.....	20
About GFI.....	21

Email is a constant. Email is everywhere. Email is something few of us can live without. Over 180 billion messages are sent and received every day, and most of us gets hundreds every week – if not every day. Each of these seemingly innocent emails could be a vector of attack, a container of malware, or a way to destroy your company's very business.

It would be easy to stop hackers if they only used email in one way to attack a company. Unfortunately, email is vulnerable in many ways and hackers have made the most of that and continue to come up with ways to use email to infiltrate an organization. And it gets worse every day.

You must protect your network from these attacks. One way is to go back to basics, and make sure you are taking all the necessary steps to fortify your email infrastructure. You must also be on guard for new and persistent attacks that require forward-looking approaches to deal with and ward off attacks on your email. Spam, is the least of your worries.

In this ebook, we lay out current situation, and give you 10 tips to deal with the problem.



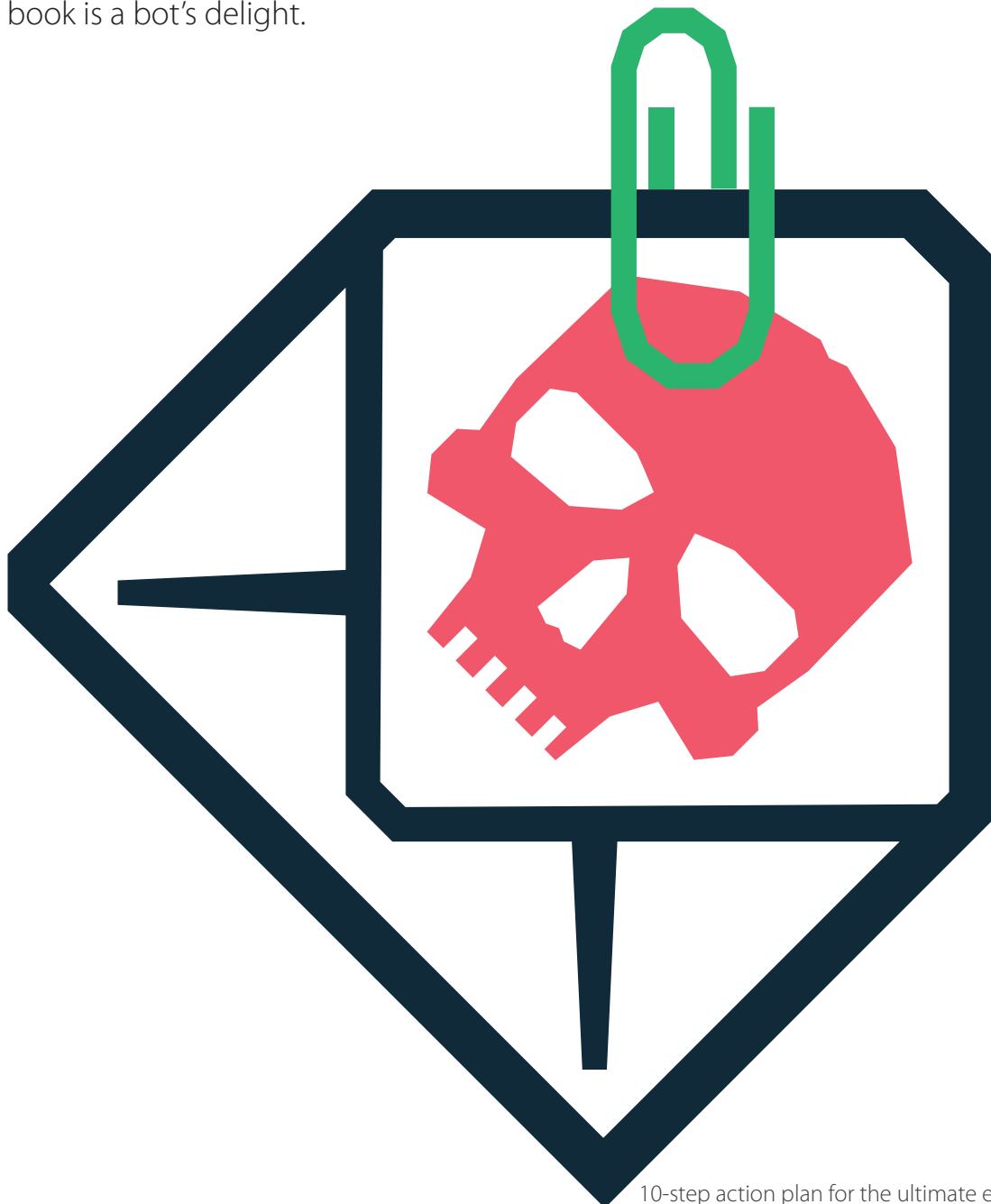
# Why is email so vulnerable?

Email is one of the easier ways for attackers to gain access to your network. Once they're in, they have the keys to the kingdom. Not only can they gain higher level access to the network, especially if they launch an elevation of privilege attack, but they can see all user's email content, and use that information to take over their identity, amongst other nasties.

Email is vulnerable. Not only are passwords commonly weak, and users are easy prey for social engineering, but controlling a user's address book is a bot's delight.

How many times have you received bogus emails from friends or colleagues because their address books were hacked? And because these emails are from people you trust, you are more likely to open them. So how easy is it for an employee with very little awareness to fall for these ploys and, say, click on an infected link?

The people behind these threats are organized, international criminals who use very sophisticated methods.



# What harm can hackers do via email?

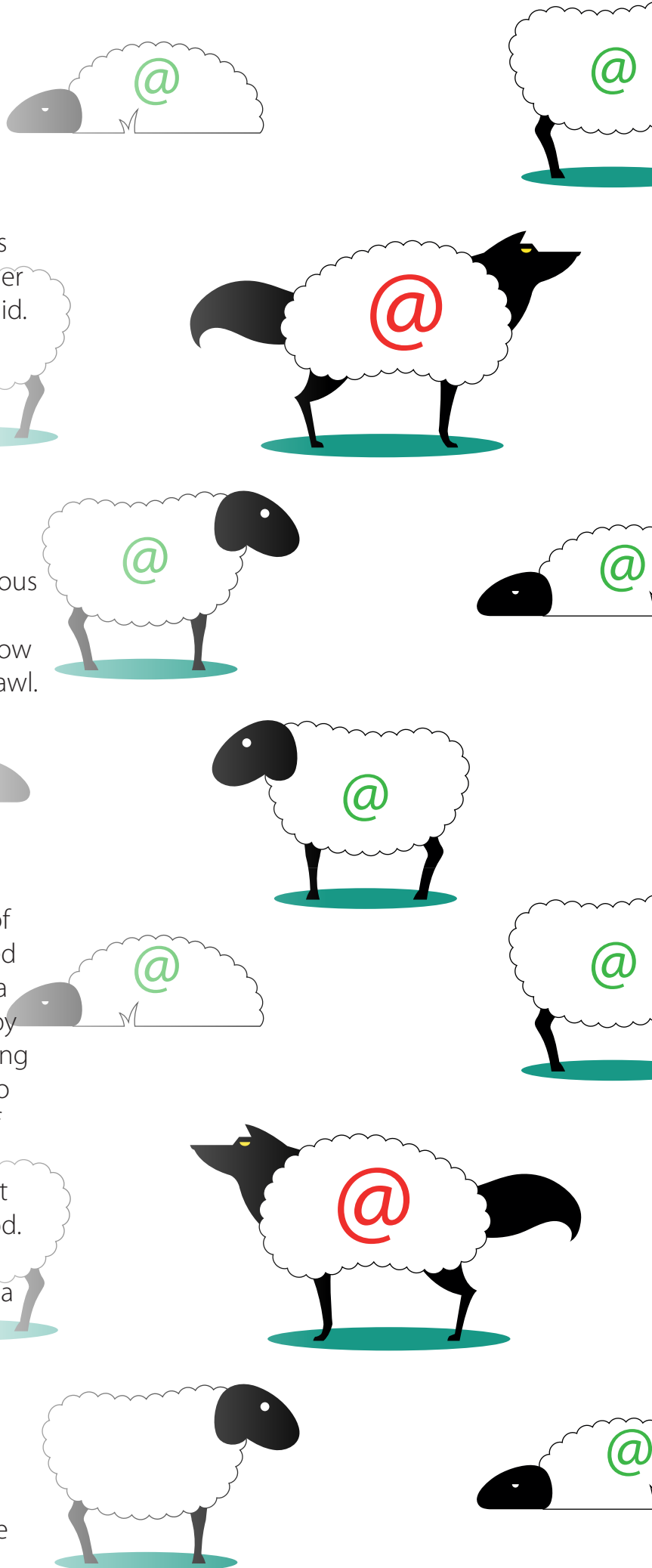
We sometimes feel certain email attacks as just annoying. So what if Aunt Betsy's Gmail was taken over by a bot and we got a bogus message? Even if you sidestepped the danger of Aunt Betsy's bogus email, not everyone did. And those who fell for it probably harmed other users, including those in your own corporate or personal address book.

The worrying thing about these incidents is that the user often only gets to know they were compromised when they get an email from their contacts pointing out the suspicious mail. And if that email account is taken over just to spread spam, the victim may only know if their machine's performance slows to a crawl.

These attacks are just the tip of the iceberg. There are many more subtle and dangerous attacks. For example, traditional style email viruses are still a massive problem.

We need to go back some time, and a few of you may remember a little nasty virus named Melissa back in 1999. Far from sweet, Melissa used email to bring systems to their knees by overloading them. The virus spread by tricking users into opening an attachment hoping to get free pornography by offering up a list of supposed passwords. The attack was finally beaten back after much harm was done, but that didn't mean the virus was done for good. To the contrary, Melissa proved to hackers what was possible, and they took the Melissa code and spread new versions.

This is one of the biggest drivers for hack attacks. The bad guys share code, and these days even a coding novice can re-launch an existing piece of malware with just a few tweaks. With Melissa, the hacker gloves were off, and email was suddenly prime game.





# Attacks broaden and worsen

Hackers love easy pickings and they more so love a target that is ubiquitous. This is why Microsoft® software has long been the biggest target. Email fits the same exact profile of near-total commonality and the typical email user is confronted by phishing, malicious links, elevation of privilege exploits, and address book attacks.

The rise of email makes it a bigger problem: today users have corporate email, but they are also likely to have multiple web mail accounts, thus multiplying the number of attack vectors. For most of us, email is the app we still spend the most time with. It is hard to keep up with the volume of legit mail, never mind the spam. So when malicious mail masquerades as legitimate, even seasoned users can fall victim.

Email is the perfect conduit for worms, a form of malware that multiplies and spreads largely through email distribution. With script kiddies, these worms never die: they are simply tweaked and turned into more dangerous entities.

Take Win32/Brontk, which has been around for years. This is a classic worm which proliferates through mass mailing. In typical fashion, this worm mails itself off with an innocent-looking email attachment, and finds addresses by hijacking end user address books. To make things worse, worms like Win32/Brontk can shut off your defenses such as anti-virus software and even use the hijacked email to launch denial of service (DoS) attacks.

Then you get money scams, similar to the well-known Nigerian scams. In one example, Mrs. Bridggie William from Kenya writes that her husband died after a “Cardiac Arteries Operation,” leaving behind over \$10 million. As Bridggie herself is dying of cancer, she wants the recipient to provide a safe place for all this money.

Instead of an email address to respond to, Bridggie was kind enough to include an Outlook meeting invitation. Acknowledging such invites can open you up to serious attacks. Of course, these meeting requests

must be deleted immediately, and not just moved to your junk folder. And just as you ought not to respond to spam, do not decline the invite as this is akin to a response.

Allowing employees to have multiple accounts multiplies the threats you need

to tackle. It is best to restrict user access to the corporate email system only while they are on the corporate network. Hopefully, defense in depth protection tools have been implemented. Unprotected accounts are also a major source of data leakage and malware.

On the other hand, if users do a lot of web surfing and sharing, it may make sense for you to help support these web email clients. They can use these accounts for non-business purposes, but still need to make sure they are protected since their use can ultimately impact the company.



# Spam still a problem, maybe more than ever

Spam, is often seen as a pure annoyance. Our inboxes are flooded with junk daily.

Spam is a main conduit for hack attacks, be it malware or phishing. And spam is more dangerous than ever. The bad guys are not just trying to lure you to buy bogus wares, but want your information, your address book, and to use your connection to elevate their privileges and attack your company's network.

According to the Microsoft Security Intelligence Report: "More than 75 percent of the email messages sent over the Internet are unwanted. Not only does all this unwanted email tax recipients' inboxes and the resources of email providers, but it also creates an environment in which emailed malware attacks and phishing attempts can proliferate. Email providers, social networks, and other online communities have made blocking spam, phishing, and other email threats a top priority," the report said.

There is far more to it than that. Spam wastes productive time as your workers pore over their inboxes and sift through the garbage. And spam is not going away. While not exploding as in years past, spam isn't exactly disappearing either. At the same time, it is getting more dangerous and laden with malware and phishing attacks every day.



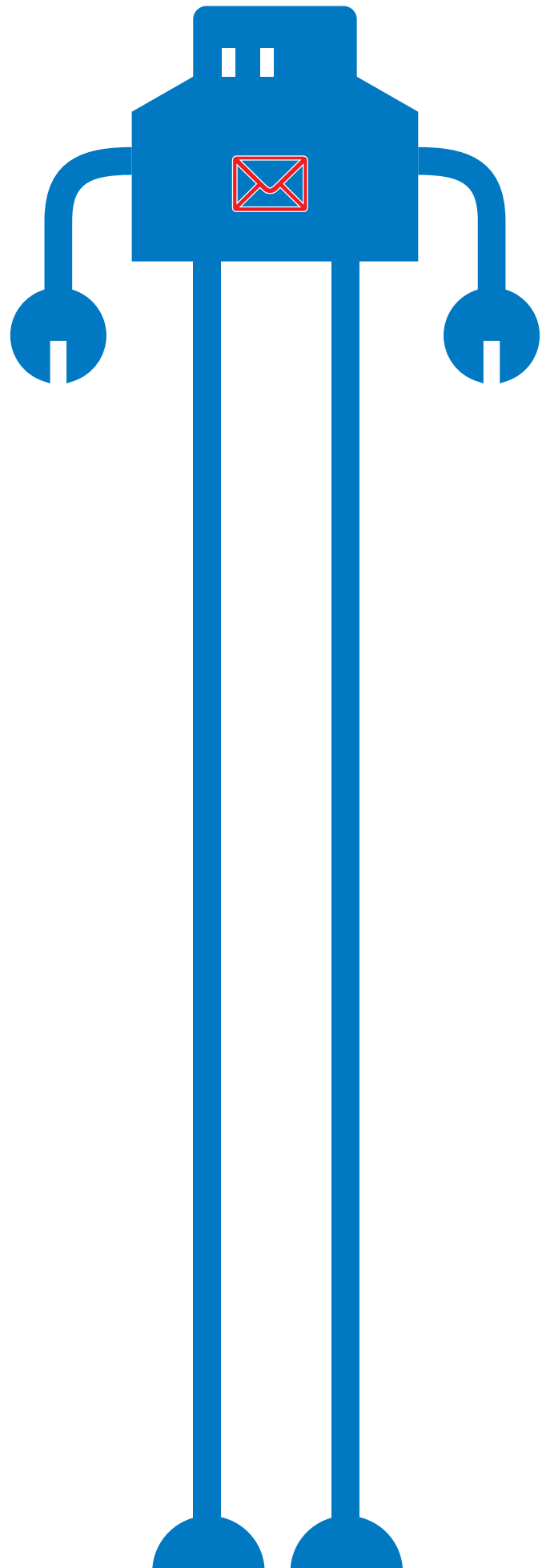
# The new ThingBot threat

When we think of hack attacks, we imagine someone behind the keyboard with nothing better to do than cause problems. But most attacks are now automated and there is a new threat. More and more small devices and even appliances are now IP devices and can communicate with each other and our networks. This is known as the Internet of Things (IoT) and machine-to-machine (M2M). The problem is that the number of devices that can be used in an attack or that can be subject to attack is multiplying at a fast rate.


Playing off the IoT term, these new attacks are called ThingBots and they use these newfangled devices to launch botnet attacks. In fact, a single botnet last year took control of over 100,000 of these small devices to spread its attack. This resulted in over 750,000 spam and phishing messages being sent out in just two short weeks.

Many types of attacks can be launched this way including malware, and the spreading of inappropriate content and spam – which comes with its own litany of troubles.

Email attacks are not only originating through our computers but there is also evidence to suggest that smart refrigerators and intelligent thermostats, our mobile phones, home routers, and other consumer electronics are fast becoming suitable conduits for attacks.








# IT'S TIME TO FIGHT BACK

Your company's network, applications and data are the lifeblood of your business. Even if compromised just a little and you are seriously damaged. Compromised a lot, and you may be down for the count. Protection is of the essence, and this protection must be deep and rich.

Here are 10 top tips and an action plan to lock down email for good.

- 
1. Demand passwords
  2. Stop data leakage with content filtering
  3. Stop spam before it really stinks
  4. Stop breaches with content filtering
  5. Make malware go away
  6. Block breaches
  7. Consider compliance
  8. Training and best practices
  9. Fight phishing
  10. Implement defense in depth

# Step 1: Proper passwords

1

What is email's first and often only layer of defense? It is often a password. And since users generally use one password for multiple apps, if that password is cracked that exposure is compounded.

Unfortunately, passwords are usually far too weak, as easy to crack as a freshly-laid egg. Even many shared accounts set by IT have insanely simple passwords. How many times has someone told you to key in "password", "admin", or "guest". Maybe if the admin is sneaky they'll have you enter "password123", "admin123", or "guest123". Like that will stop a motivated hacker!

Another good practice is to have different passwords for different emails and other accounts, so if one gets discovered, the others aren't found out as well. If you decide to go with just one master password, make sure it has a high level of complexity and is changed regularly.

Making matters worse, email is not just email any more. It often has integration and links to Facebook and other social media, and at the very least, notifications from services such as LinkedIn, Amazon or eBay that can reveal a lot about the user. If a hacker is in your email, the first thing they will do is see if your password works with these other services. If it does, they know enough about you to make identity theft a breeze, or use this information to launch false personal attacks and create other mischief.

These attacks can easily come from people you know. If they have your email address and know you love Harley-Davidson motorcycles, they might figure out after a few attempts that your password is harley1234 or something similar. Jilted lovers are just another example of those who would do such a thing.

Your users need complex passwords that are changed regularly. Even more so, they need a safe way to store passwords, as complex passwords are easy to forget. Having them in an encrypted file is best. Make sure they never write them on a Post-It note and stick it to their computer, the back of their monitor or leave it in their top drawer.

We tend to think that it is end users that are the real risk, but a 2013 survey by Ping Identity found that 83 percent of security pros use one password to use multiple applications too. Trustwave, a security consultancy, looked at millions of passwords that had been compromised and found that, in most cases, the passwords were far too weak. Half of these passwords had low level security, but in many cases had at least a number combination and upper and lower case letters which isn't horrible. Close to 90 percent of the passwords had no special characters. Even worse, the most popular password today remains "Password1", which is almost as bad as "admin" or "guest".

**"Your users need complex passwords that are changed regularly"**

## Step 2: Block data leakage

2

Data leakage is a huge and growing problem. Confidential corporate data is leaked out, as are credit card numbers, social security numbers and sometimes medical information.

What you really need is a policy that dictates that this information, under no circumstances, should be sent out without explicit management approval.

You need a tool that checks for keywords that would indicate that inappropriate data is going out the door. This keyword scanning should apply to both the emails themselves (social security and confidential are two examples of terms to look out for), as well as attachments. You don't want your Q4 numbers sent out to a broker before they are announced, do you?

The scanning really needs to be configurable to search deep into the messages, such as scanning the subject line, message body, headers and content. And like spam and anti-malware where you want multiple engines, you want a content tool that employs a variety of pattern matching techniques.

Data leakage comes in three main forms – inadvertent, on purpose by the end user, and on purpose by a hacker. In any of these cases, confidential data can be compromised. Competitors can get your financials or intellectual property, and thieves can get customer's personal information.

Data leakage can be just as dangerous as an overt outside hack. Sometimes your end users will inadvertently email confidential data. Sometimes they also misuse distribution lists and mail private information to dozens, perhaps hundreds, of recipients.

Other times, the employee leaks data on purpose, and the biggest conduit is the easiest, most ubiquitous form of communication – email. Let's face it, no one is going to text confidential company plans, it just isn't workable.

The 2015 Verizon Data Breach Investigations Report shows that 20 percent of all data breach incidents come from insiders, and because these insiders have company knowledge and already have network access, they can do more damage than a hacker which might now know where to look for confidential information. This includes skimming and distributing credit card information, selling private medical data, giving employee lists to recruiters, or selling confidential plans and results.

**“Data leakage comes in three main forms – inadvertent, on purpose by the end user, and on purpose by a hacker.”**

## Step 3: Stop spam before it really stinks

Did you know that in 2014, seven percent of all security threats came from spam carrying malware; up from three percent the year before? That ten percent of all spams harbor malicious URLs? And that last year, spam hit its highest level since 2010?

Spam is not just a nuisance, but a real danger to your business. Spam is a huge productivity waster, so is the ROI to get rid of it. Ferris Research took a look at this issue, and in one analysis assumed that if the end user received five spams a day, and spent just 30 seconds on each message, that would total 15 hours a year. Shops without proper anti-spam protections can be pretty much assured of getting a multiple of this amount of spam every day, and consequently will waste far more employee time.

Other spam costs include the price of bandwidth to transmit these worthless messages –and disks or online storage to hold them.

So what do you do to stop this scourge? Some of it is technical and some is policy-based or accomplished through training.

One technique is to keep email addresses under a tight lid instructing users not to give them out willy-nilly and post them on any website that comes down the pike. It might make sense to have a corporate policy that restricts where email addresses can be posted.

Teaching users to take maximum advantage of spam filters and be careful of how they deal with the messages in the junk mail folder is another way. Make sure they never ever open or respond to spam. By opening them, you are inviting a malware or phishing attack, and by

responding they are simply proving that your email address is valid, and that you are a good target.

Finally, make email addresses complex enough that they are difficult to guess at.

**“Spam is not just a nuisance, but a real danger to your business. Spam is a huge productivity waster, so is the ROI to get rid of it.”**

## Step 4: Controlling content via filtering and monitoring

IT and upper management know that company data is their most precious resource, and some data is more precious than others, such as financials, client data, unreleased products, strategies – all of which are all game changers if stolen. At the same time, inappropriate content is yet another risk.

While many believe the only real security threat comes from outside hackers, the insider threat can be more insidious and dangerous. And with email, your end users don't even always know they are causing such a problem.

Some of these problems are the inadvertent spreading of malware or exposing corporate data by falling prey to phishing.

Another problem has to do with employee misbehavior and here is where email content monitoring and control can be a lifesaver. There are myriad ways these bad deeds can bite you; data leakage, criminal complaints if email is used to break the law, and lawsuits if an employee, for instance, uses email to sexually harass someone.

More and more often, courts are ruling that organizations are responsible for what happens on their systems, including email. Email content monitoring can help solve most of these problems, keeping your company out of hot water by blocking inappropriate messages. Email content monitoring can also help ensure compliance regulations are met.

Frost & Sullivan studies this market, and recently did a survey of 12,396 security pros which informed its Analysis of the Global Web and Email Content Security Market report.

One key is for vendors to integrate email content with other security tools, easing management and licensing. "As common intellectual property for content security is spread across communication channels like web, email and social media, vendors will be driven to offer a unifying suite of content security products with a single point of interface. As such, market consolidation will reduce complexity for customers and decrease administrative overheads for security professionals," said Frost & Sullivan Network Security Industry Principal Frank Dickson.

The need for this kind of tool is driving the market to grow from \$3.07 billion in 2013 to \$3.35 billion in 2017.

**"While many believe the only real security threat comes from outside hackers, the insider threat can be more insidious and dangerous."**



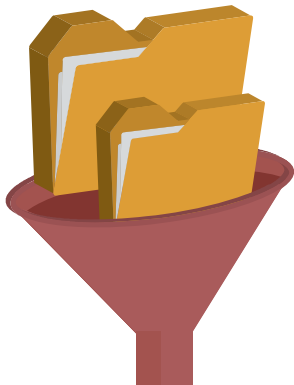
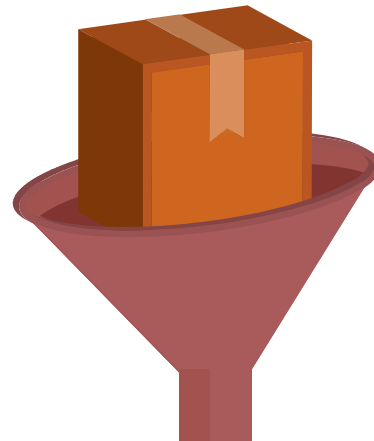
## Step 5: Make malware go away

Malware of all shapes and sizes isn't going away, but instead is getting more vicious and numerous. New attacks are coming out all the time and not only do you have to beat back the thousands of exploits already out there, you also have to protect yourself from zero-day exploits.

Just like with spam, you need multiple antimalware engines for true protection.

Content filtering is another way to fight zeroday attacks. Good filtering will recognize and block the types of attachments likely to carry a viral payload.

5



**“Good filtering will recognize and block the types of attachments likely to carry a viral payload.”**





## Step 6: Block breaches

6

Every year Verizon studies breaches in its Data Breach Investigations Report. One disturbing finding is that email attacks are being used more and more for espionage, and these can be launched by criminals or state-supported organizations. In the 2015 Verizon Report, 0.8 percent of all data breaches were due to cyber-espionage.

Some attacks are in the form of a phishing email; once you click on a link or links, even more malware is downloaded onto the user's computer. The goal is to let the hacker gain domain level access which it can do by capturing credentials, installing a key logger or another technique.

"Throughout this process, attackers promulgate across the systems within the network, hiding their activities within system processes, searching for and capturing the desired data, and then exporting it out of the victim's environment," Verizon said.

Verizon further finds that email remains the most popular way to launch social attacks, with phishing being the most frequent.

**"email remains the most popular way to launch social attacks, with phishing being the most frequent."**

**SOS**



# Step 7: Compliance

7

All these issues are more serious for those companies covered by compliance regulations where you must beyond a shadow of a doubt prove that your email, and the data it contains, is safe.

Here, you must protect all aspects of your mail and insure that your key corporate data, be it credit card numbers, personal information, or financial information. Fortunately, the same basic protection techniques that serve those ordinary shops can also protect those that fall under compliance.

Compliance isn't just a guideline, but a mandate. Take the Health Insurance Portability and Accountability Act of 1996 (HIPAA), for example. Here violating compliance rules can mean real dollars.

These fines can start out relatively small, but are nonetheless painful. For instance, in Idaho, a hospice had a laptop pilfered. Despite all the hospice's good deeds, it was still fined a stinging \$50,000. In Phoenix, Insecure email cost a small medical practice a cool \$100,000.

That's the small potatoes. In Boston, a misplaced physicians' laptop – just that one computer – netted a \$1 million fine. Even state government isn't immune as the Alaska State Health Department lost just one backup drive, which cost them \$1.7 million.

Email creates this kind of compliance exposure thousands of times a day, especially when it becomes a source of data leakage.

For instance, an employee of The Regional Medical Center in Memphis mistakenly sent out email with patients' private medical information. Even though an accident, the center had to warn hundreds of people of

the compromise. No big deal? Close to 1,200 patients had their records compromised, and that data included not just medical history but also personal information such as social security numbers, a hacker's goldmine.

**“Compliance isn't just a guideline, but a mandate.”**

## Step 8: Training and best practices

8

IT is used to deploying technology to solve technical problems, so they implement firewalls, anti-malware and other devices. Unfortunately, these defenses aren't always rich or deep enough.

Just as large an issue is end-user behavior. All the defenses in the world can't defend against an easily fooled employee who may be tricked into giving a hacker full network access.

Training clearly pays off, especially in blocking phishing, and perhaps no one knows this better than famed hacker Kevin Mitnick who now works for security training company KnowBe4, LLC. This company spent a year studying 372 shops representing some 291,000 endpoints.

Before training kicked in, nearly 16 percent were prone to falling for phishing attacks. After training, that fell by a factor of 12, down to just 1.28 percent. KnowBe4 believes the real weak security link is end users.

"The threat posed by malware should not be underestimated, particularly considering that employees have consistently proven to be the weak link in companies' Internet security efforts," Mitnick said. "In most cases, their involvement is unintentional – they unknowingly allow access to corporate networks simply because they don't know what to watch out for".

A properly trained employee, on the other hand, can act as what Mitnick calls a 'human firewall'.

Some scams never die because they are so darn enticing that they just keep on working, and not enough users are trained to avoid them. Most by now can at least spot the old

Nigerian scam. But the lure of money keeps lottery scams going and here the trusted names of Microsoft and Google are often used. Instead of Nigeria, which nowadays immediately raises suspicions, these messages want users to contact someone in England or another industrial country.

Microsoft in particular is keen to stop these scams, so if you get one of these messages, by all means contact Microsoft. In fact, Microsoft is one of many vendors that work closely with law enforcement to hunt down and punish criminals.

**"Before training kicked in, nearly 16 percent were prone to falling for phishing attacks. After training, that fell by a factor of 12, down to just 1.28 percent."**

# Training tips and tricks for your users

- Never click a link in an email you aren't 100 percent certain is legit.
- Never respond to spam.
- Never open an attachment unless you asked for it or know precisely what it is. And don't be fooled because it looks like a Word doc or some other seemingly innocent file. It is a piece of cake to change an .EXE extension to .DOC.
- Never interact with an email from a business you weren't expecting. Even if a message seems to come from your bank, ignore it and use the website, protected by your password and user name to see if there is anything you need to tend to.
- Use professional-grade spam filters, and make sure the settings and quarantine policies meet your needs.
- One phishing technique is to lure you to an actually legitimate site, but once you get there, a malicious dialog pops up asking for personal information. Resist the urge to fill in any data. Activating your browser's pop-up blocker might help.
- If you think you clicked a bad link or did something else to launch an attack, either start a scan immediately or shut down the machine and immediately get help from an IT professional before the problem spreads
- Set up your anti-malware to run regularly, keep it updated, and do a full scan immediately if you suspect trouble.
- Be wary of public Wi-Fi. Try to keep to trusted providers, and take immediate steps if you sense your computer has been compromised. Hackers often use network sniffers to study your connection, and nab user names and passwords.
- Consider a separate, non-corporate email account for personal use, but treat this with the same respect as you do corporate email, and try to not to use it while on the corporate network
- Be wary of sharing your address by posting it on forums, blogs, and websites as hackers can scrape these sites and add you to their spam list. If you feel you must share, use a personal email address rather than your corporate account.
- Keep applications and apps updated and patched.
- Use legitimate (non-pirated) software.
- Make sure an attachment is legit before you open it.
- Don't open unusual messages, even from friends, family, and colleagues.
- Report phishing and other attacks to key vendors and security firms.
- If you get an unexpected calendar invite, delete and contact the sender, if you know them, to see if was legit. If so, have it resent. Never respond to these invites.

## Step 9: Fight phishing

9

While most phishing attacks target consumers, some are after richer quarry. In February 2015, right in the midst of US tax season, a phishing attack targeted tax professionals, asking them to update their electronic filing information. The real goal – to steal user names and passwords and get information on thousands of potential tax claims.

This is only the tip of the iceberg – and phishing is on the rise – especially in terms of the level of sophistication.

In the last couple of years, nearly 40 million users were hit by phishing, and this is a nearly 90 percent increase from the two years prior.

Phishing all too often works, and that's why the bad guys are so persistent in sending it. In fact, even if the first attempt doesn't work, there is a good chance the second or third will, according to findings by Verizon. Referring to research from ThreatSim, "running a campaign with just three emails gives the attacker a better than 50 percent chance of getting at least one click. Run that campaign twice and that probability goes up to 80 percent, and sending 10 phishing emails approaches the point where most attackers would be able to slap a 'guaranteed' sticker on getting a click," Verizon said.

Training to spot phishing is one half of the prevention equation. The other half is strong tools that can spot and block phishing messages.

The Microsoft Security Center wants users to avoid phishing, and gave this annotated phishing example to help. Things to look for include bad grammar and incorrect spelling, something especially found in phishing messages from China and Eastern Europe.

And, of course, links in the email can be another tell-tale sign. Even more telling are messages that threaten to close your account or take some other form of action if you don't respond.



# Step 10: Implement defense in depth

Training users to spot malicious mail and social engineering attacks is critical, but even more so is having proper technical defenses. That means protections against all forms of intrusion and data leakage.

## And that means having:

- Antivirus/anti-malware
- Spam protection
- Content filtering

It is best if all these tools are integrated, and offer the choice of running them in the cloud or on premise. On the malware and spam protection front, you also want to make sure that there are multiple engines that are updated frequently so that nothing gets through.

The return on investment (ROI) on email security isn't a precise measurement, but it is assuredly positive and fast. If you block just one major attack, which you most probably will, the ROI will be off the charts. At the end of the day, you need to ask yourself, how much is my business worth?

## Integrated tools

Fortunately GFI Software™ has the technology that offers this defense-in-depth.

GFI offers GFI MailEssentials®, which has three versions ranging from full-on unified protection with anti-virus/anti-malware, and spam protection; an anti-spam/anti-phishing edition; and an anti-virus/anti-malware tool.

On the malware side, GFI MailEssentials can offer five powerful anti-virus engines which scan your emails for potential exploits.

In addition, GFI MailEssentials can sanitize, or in other words cleanse the HTML code of malicious scripts in email before it is transmitted, possibly causing an infection.

Users should also know how to protect themselves, which is where training from IT comes in. GFI adds to that tools that let end users manage spam quarantines, whitelists and blacklists. Even better, the GFI tool catches more than 99 percent of all spam messages. And don't worry about your legitimate messages not getting through. GFI MailEssentials is regularly awarded the VBSpam+ award for its 0 percent false positive rate.

Tracking content and enforcing policies is also critical, and here GFI MailEssentials lets IT set policies based on groups or users, and rules can be based on email headers, keywords or attachments.

And all this management is eased for IT through a web console, which includes powerful integrated reporting. Finally, the software is only installed on the server, with no need to install client applications.



## GFI can help you

Block out spam and take control of your email security with GFI MailEssentials™

Try **FREE** for 30 days



Learn more



## About GFI

GFI Software™ develops quality IT solutions that enable businesses to monitor, manage and secure their networks with minimal administrative overhead. Serving an expanding customer base of tens of thousands of companies, GFI focuses on scalable communications and security platforms comprising network security, web management, anti-spam, patch and vulnerability management, faxing and archiving solutions. GFI is a channel-focused company with thousands of partners worldwide. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.



[www.gfi.com](http://www.gfi.com)

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

Other email and messaging solutions from GFI

**GFI Archiver™**

*Archiving for productivity, management and compliance*

**GFI FaxMaker™**

*Network fax server software for Exchange/SMTP/Lotus*

**GFI FaxMaker™ Online**

*Simple, fast, online faxing*

Disclaimer. © 2015. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.