

WHITEPAPER

Stop Email Fraud
...Before it Stops You

Table of Contents

1. When Email is the Enemy	1
2. Three Things You Need to Know about Email Fraud	3
The Fraudster	3
The Frauds	4
The Facts	5
3. Four Steps to an Effective Anti-fraud Solution	6
Detect	6
Protect	6
Align	6
Inform	7
4. Conclusion	8
5. About MailFrontier	9

1. When Email is the Enemy

Of the many types of unwanted email that threaten your business today, spam gets most of the attention, and rightly so. More than 70 percent of email sent in the United States is commercial spam. But email threats come in many forms and new types can appear at anytime, limited only by the imaginations of their perpetrators. In fact, some of the most malicious email threats aren't just carried in an email message—they are *the email message in the form of fraudulent emails.*

Until recently, email fraud was a problem for consumers. According to an April 2004 report from Gartner Group, an estimated 57 million Americans think that they have received a phishing email. And the problem is growing. A study by the Anti-Phishing Working Group showed that between November 2003 and April 2004, phishing emails—the most common type of fraudulent email—increased 110 percent each month. With the average successful fraud netting \$1,400, consumer email fraud is already a \$5 billion industry.

Every company is vulnerable to email fraud.

Flushed with success defrauding consumers, fraudsters now are turning their sights on businesses—discovering that techniques that work well with consumers work equally well with unsuspecting employees. Fraudulent emails aimed at employees often appear to come from trusted sources such as company management or partners; use legitimate company graphics, layout, content and links; and ask employees to take actions that seem reasonable in a business context, such as verifying company information.

Financial services, insurance and health care companies – all keepers of sensitive information—are especially prime targets for email fraud attacks and the stakes are high because regulators hold them to stringent privacy and security standards. *But the truth is every company is vulnerable to email fraud attacks and every attack has the potential to create devastating losses.*

In addition to time and money, one of the most significant losses stemming from email fraud is *trust*. Even a single successful email fraud attack renders your email system untrustworthy, transforming one of your most valuable business applications into one of your most serious business threats.

Email fraud attacks are an especially thorny problem for growing businesses. The impact of an attack can be just as devastating to you as it is to large enterprises, yet you may lack the financial or technical resources to fight back effectively.

In this whitepaper, MailFrontier—an innovator in email security that protects growing organizations from spam, virus and fraud and other email threats—levels the playing field for growing businesses concerned about the escalating problem of email fraud. In addition to three things you need to know about email fraud—including three common myths—MailFrontier outlines four steps growing organizations can take to an effective anti-fraud solution.

You are at risk; but you can do something about it.

2. Three Things You Need to Know About Email Fraud

To effectively combat email fraud, there are three things you need to know about it: The fraudster, the frauds and the facts.

The Fraudster:

The Spammer's Bigger, Badder Alter Ego

Many organizations treat email fraudsters as "just another spammer" and in some ways, fraudulent emails do look and act like spam. They come in unsolicited and tend to request something of the recipient such as a purchase, an action or an entry of information. But the similarity ends there. While spammers send junk mail that is often blatantly authentic, fraudsters cloak themselves in the guise of partner or friend. While the spammer seeks attention, the fraudster avoids it, masquerading as a trusted source and using your corporate email system and your employees against you.

Meet the fraudster, avoid the fraud know, the facts.

And while neither the spammer nor the fraudster is welcome on your corporate email system, the fraudster is by far more threatening. While a little spam might be annoyingly but acceptable, a little fraud is totally unacceptable. A single successful instance of email fraud could expose your corporate network, corporate data, employees and customers to the criminal or malicious imagination of every hacker and criminal on the Web. Even if the hole is patched almost immediately, there might be time enough for a fraudster to harvest an entire database of customer credit card numbers and destroy your reputation.

The Frauds:

Phishing, Bogus Updates and Billing Fraud

The three most common types of fraudulent emails are phishing, bogus updates and billing frauds.

Phishing

Phishing expeditions give fraudsters a new trick to hook unwary marks by leveraging their confidence in recognized brands and trusted sources. While phishing is usually considered a consumer issue, the

Fraud top three:

- Phishing
- Bogus updates
- Billing fraud

fraudulent techniques they use are now emerging in the corporate sector. Like their consumer counterpart, enterprise phishing emails also appear to come from trusted sources, such as company management, your IT department or a business partner. They inform the recipient that updated information is needed immediately to keep an account open or maintain network access. They usually include a link to a “spoofed” or fake Web site. Sometimes, the link may be to a legitimate site, but a spoof pop-up appears on top of it. Simply by following directions, the employee unwittingly provides the fraudster with sensitive financial data or network access information. With your corporate network compromised, you have no choice but to recall and reissue all secure ID badges, check all devices for malicious software and trace all account activity for evidence of unauthorized activity.

Bogus Updates

Another form email fraud attack is the bogus update. Among the most common types of bogus update is the software update—a fraudulent email that informs your employees of the availability of new versions of software and sends them to spoofed Web sites where they unwittingly download malicious code. Bogus updates persuade employees to take actions they would never consider if they knew the true source.

Once in a system, the malicious code can attack in a number of ways. It can bypass security protocols to obtain enterprise information; damage hard drives past recovery; steal email addresses for mass mailings of malicious messages; or infect other users through chat sessions. Sometimes a machine can be compromised even without downloading a program or executing an attachment: Simply opening the email sometimes is enough to take down an entire corporate network.

Billing Fraud

Fraudulent billing emails take advantage of the fact that no process or person is perfect. Every day in accounting departments around the world, accounting staffs process billions of dollars in legitimate business payments. When an account falls behind, sometimes a vendor sends an email notice, which in turn prompts someone in accounting to process a payment as directed. Sometimes, to expedite payment, accounting may use a corporate credit card to pay the bill online.

By closely mimicking the look and feel of a trusted vendor or partner, fraudsters use fraudulent billing emails to obtain credit card information, illegal payments or both. In extreme cases, fraudsters change your processes for electronic invoicing, re-directing all payments to a particular vendor to the fraudster instead.

Meet the myth.

The Facts:

Current Protections Won't Stop Email Fraud

Businesses are well aware that email threats such as spam and viruses can cripple productivity, increase liability and cause IT costs to skyrocket. As a result, they have invested millions of dollars in anti-spam and anti-virus protections.

- **Myth #1: The best way to prevent email fraud is to stop fraudulent emails just as you stop spam—with your spam filter.**

Fact: Fraudulent emails are specifically created to imitate legitimate emails. They are well-written, business-oriented emails from an apparently trusted source—exactly what anti-spam filters must allow into your organization. Some fraud emails carry out this deception so well that they consistently elude spam filters. While it is tempting to equate the two, fraud is not spam. Fraud requires specific analysis, identification, and handling in order to keep it from having a negative impact on your organization.

- **Myth #2: Identifying fraudulent email is simple—just use digital certification, encryption, or sender identification to confirm all sources of email.**

Fact: Digital certification and encryption are useful techniques for identifying fraudulent emails, but they are costly and time-consuming to deploy for even the largest enterprises and cost-prohibitive for smaller organizations. Authentication of the email sender could help reduce fraud eventually, but its protocols are still in development and years from a simplified, standardized implementation.

- **Myth #3: If verification technology fails, our employees can be trained to recognize fraudulent emails.**

Fact: You cannot count on the abilities of your employees to distinguish legitimate content from its fraudulent twin. MailFrontier Research shows that 28 percent of people shown fraud samples will misidentify them as legitimate. Furthermore, 1 in 10 people will act on a fraudulent email even *after* they have been told it is suspicious.

3. Four Steps to an Effective Anti-fraud Solution

Four steps to stop fraud:

- Detect
- Protect
- Align
- Inform

An effective anti-fraud solution combines innovative tools and techniques specifically designed to combat fraud with consistent and accurate communication. MailFrontier recommends four steps: Detect, protect, align and inform.

Step #1:

Detect. Use analysis techniques specifically designed to detect fraud

Spam filters, which are specifically designed to let legitimate email into your corporate network, will not stop fraudulent email that looks identical to the real thing. An effective anti-fraud solution must be able to analyze a variety of message attributes that set fraudulent email apart from spam and legitimate email—including sources, formats, structures and content—and make definitive judgments about authenticity.

Step #2:

Protect. Develop containment and control protocols specifically for fraudulent email

Fraudulent email is not spam. It should not be placed into quarantine with spam and allowed into your corporate network where your employees might remove it from quarantine and act on it. An effective anti-spam solution must be able to segregate fraudulent emails immediately from other types of unwanted email and offer your IT department the option of deleting them at the perimeter of your network, before they have a chance to reach any recipient. In fact, MailFrontier strongly recommends that only members of your IT staff are authorized to view and delete fraudulent email once it has been identified and segregated.

Step #3:

Align. Make your anti-fraud solution is part of an overall email security solution

Your anti-fraud solution should not stand alone. An effective anti-fraud solution should offer a number of options that align with other corporate security processes. Your legal department may want a paper

paper trail of all attempted fraud attacks, while corporate security may want alerts about new types of fraud as they emerge. Your anti-fraud solution also should be linked into a greater network of security entities outside your business that send out regular alerts about emerging fraud techniques, giving your IT department the best possible information and the longest possible lead time to build new defenses before a new fraud outbreak hits you.

Step #4:

Inform. Increase awareness and communication about email fraud throughout your organization

The more your employees know about how they are being targeted and what they should do when they suspect email fraud, the more likely they are to take appropriate action when you are hit by fraud. An effective anti-fraud solution needs distinct fraud reporting, alert and feedback tools, so that administrators can be kept aware of trends, make necessary modifications at the network level and report those findings back to other entities that are part of your security network both inside and outside your organization. Alerts should be educational, instructional and should heighten awareness and caution. Encourage your employees to report fraud or suspected fraud. The more you know, the better prepared you can be

4. Conclusion

Fraud is not new and businesses have fought the fraudster since the beginning of commerce. But just as business practices evolve to keep pace with emerging technology, fraudsters also adapt to the new opportunities that technology offers. Nevertheless, by understanding email fraud as a distinct and more sophisticated type of email threat, and by seeking solutions designed specifically to stop fraudulent email, you can protect yourself.

While specialized applications to prevent spam and virus attacks are available, a solution that integrates anti-spam, anti-virus and anti-fraud detection makes the most sense. Not only does an integrated solution reduce administration and increase efficiency, it also allows you to analyze the sources of greatest threat to and respond accordingly. Most important, all elements of an effective anti-fraud solution should be transparent to your employees and performed automatically at the perimeter of your network.

Fraud is not new. Business has fought the fraudster since the beginning of commerce. And just as business practices evolve to keep pace with emerging technology, fraudulent practices also adapt to the new technological opportunities that present themselves, especially in this age of electronic communication. However, by remaining aware of fraud as a distinct and more sophisticated type of email threat and by seeking solutions designed specifically for fraudulent email issues, IT professionals can be well-prepared and well-positioned to ensure that their enterprise is not taken in by the eye-catching handiwork of fraudsters, disguised as gift or gain and invited in unawares.

About MailFrontier

MailFrontier guards the perimeter of the enterprise against the costly, dangerous, and growing threats to corporate email. Threats are stopped before they infiltrate corporate mail servers and employee inboxes. MailFrontier secures company connections and blocks unwanted email while ensuring timely delivery of all legitimate email. MailFrontier Enterprise Gateway™ provides comprehensive protection against fraud, spam, directory harvest attacks, viruses, and email policy violation. The solution is dynamic, self-learning, and self-running, providing IT departments with the hands-off protection they need. MailFrontier Enterprise Gateway offers redundancy, comprehensive reporting, and central administration across multiple data centers. The solution scales for enterprises of over 100,000 employees. Fortune 1000 businesses across virtually every industry protect their email with the MailFrontier solution. Industries include media & entertainment, insurance, financial services, utilities, healthcare, manufacturing, high technology and other sectors. MailFrontier customers include Pier 1 Imports, Wyndham Hotels & Resorts, and Peet's Coffee & Tea.

**Keep your email system safe.
Keep your employees productive.
Make email good again™.**



For more information about MailFrontier Enterprise Gateway, the most extensive email security solution designed for the enterprise, please contact us at sales@mailfrontier.com

1841 Page Mill Road
Palo Alto, CA 94304
866-3NO-SPAM