

This Free E-Book is brought to you by [Natural-Aging.com](http://Natural-Aging.com).

**[100% Effective Natural Hormone Treatment](#)  
Menopause, Andropause And Other Hormone Imbalances  
Impair Healthy Healing In People Over The Age Of 30!**

## Why Corporations Need to Worry About Phishing

By CipherTrust

### Why Corporations Need to Worry About Phishing by CipherTrust

Phishing is a relatively new form of online fraud that focuses on fooling the victim into providing sensitive financial or personal information to a bogus website that bears a significant resemblance to a tried and true online brand. Typically, the victim provides information into a form on the imposter site, which then relays the information to the fraudster.

Although this form of fraud is relatively new, its prevalence is exploding. From November 2003 to May 2004, Phishing attacks have increased by 4000%. Compounding the issue of increasing volume, response rates for phishing attacks are disturbingly high, sometimes as high as 5%, and are most effective against new internet users who are less sophisticated about spotting potential fraud in their inbox.

Corporations should be concerned with the following four issues:

- Protecting employees from fraud
- Reassuring and educating customers
- Protecting their brand
- Preventing network intrusions and dissemination of trade secrets

A failure to succeed in any of these areas could be catastrophic to a company's ability to function in the marketplace. If employees are not protected, the company could be held accountable for not putting protections in place to prevent fraud. If a hacker impersonates a company, then the company's reputation and brand may be tarnished or ruined because customers feel that they can no longer trust the organization with their sensitive information. And finally, the latest trend in phishing has been to socially engineer employees or business partners to divulge sensitive trade secrets to hackers. The implications of employee login information getting into the wrong hands could result in grave consequences once hackers are able to "log in" to an employee's network account using VPN or PC Anywhere software.

Protecting Employees from Phishing

## Why Corporations Need to Worry About Phishing

One of the best ways to protect employees from Phishing is to prevent spam from ever getting to the user's inbox. Since most phishing attacks proliferate through unsolicited e-mail, spam filtering technologies can be very effective at preventing the majority of phishing attempts.

New technologies are also available to help prevent phishing. One such technology offered as a standard by Microsoft and supported by CipherTrust is the Sender ID Framework (SIDF), which prevents spammers from obfuscating their IP address by verifying the source of each email.

Of course, spam filtering and SIDF cannot solve the problem entirely. Many phishing attacks are actually sent on an individual basis to users not protected by cutting edge spam detection technologies. Other attacks are distributed through online email accounts such as Yahoo! Mail, Gmail, MSN, and others. In short, technology alone cannot solve the phishing problem. Employees must be educated about phishing and how to spot fraudulent emails and websites.

### Reassuring and Educating Customers

Once a consumer receives a fraudulent email that appears to come from a trusted company, he or she may never trust that company's email communications again. That is damage that is not easily undone. It is essential that organizations communicate openly and frequently about how customers can identify legitimate email communications, and the need to report fraudulent ones. For those organizations that frequently process consumer credit card transactions, it is recommended that a special section of the site be devoted to helping customers avoid fraud.

Companies that make efforts to educate their customers about phishing are much less attractive targets than those who make no efforts at all. Some examples of organizations that have developed extensive policies around this issue are:

### Protecting the Company Brand

Each time a phishing attack is launched, a legitimate company's trademark is tarnished and brand equity is eroded. The more attacks a company suffers, the less consumers feel they can trust the company's legitimate email communications or websites. The value of this trust is difficult to quantify - at least until a company begins to lose customers. When customers no longer trust the company's ability to protect their personal information, they often defect to competitors or opt to use more expensive commercial options such as telesales or retail locations.

Clearly the goal is to convince the fraudsters that your customers will not fall for the scam. This is why having an obvious anti-phishing program that is public for all to see can be very effective. The fraudsters tend to follow the path of least resistance. Seeing that customers are well informed of how to avoid phishing attacks, the perpetrators simply turn their attention to other "softer" targets.

### Preventing Network Intrusions and Dissemination of Trade Secrets

Employees must be educated not only about phishing generally, but also about how fraudsters might use social engineering and other methods to entice employees to divulge sensitive information to

## Why Corporations Need to Worry About Phishing

hackers outside the organization.

With little knowledge of an organization's business methods, hackers can easily distribute hundreds or even thousands of spoofed messages to an organization's employees. The messages may ask for network passwords and usernames, or may attempt to fool employees into providing sensitive information to competitors.

It is important to properly train employees about what information is appropriate to share through email, and specifically what steps employees should take if they are unsure about the authenticity of a request for information.

Information gleaned by fraudsters from corporate networks can be used in a variety of nefarious ways. In the financial services industry, criminals can use credit cards to deduct money straight from accounts of unsuspecting victims. Many other organizations hold private healthcare information, or personal financial information that could be used by criminals to extort payoffs from corporations wishing to avoid the bad publicity of a security breach becoming public knowledge.

Though deflecting this attack does involve a significant amount of education, providing content filtering on outbound e-mail traffic can flag suspicious communications. Looking for these regular expressions, like social security numbers and account numbers, can prevent a simple deception from becoming a major liability issue.

### What to Do If You Are the Victim of a Phishing Scam

If you become aware of fraudsters imitating your organization to commit phishing fraud, you should:

Immediately educate your customers on how they can correctly identify the phish  
Notify the authorities of your situation. Phishing Fraudsters may have violated all or some of the following Federal Laws:

- 18 U.S.C. 1028(a)(7) - Identity Theft
- 18 U.S.C. 1343 - Wire Fraud
- 18 U.S.C. 1029 - Credit-card Fraud
- 18 U.S.C. 1344 - Bank Fraud
- 18 U.S.C. 1030 (a)(4) - Computer Fraud
- 18 U.S.C. 1037 - CAN-SPAM Act
- 18 U.S.C. 1028(a)(5) - Damage to computer systems and files

Prosecute the criminals - when Spammers use your trademarks to commit fraud, they are violating U.S. Trademark laws as well as anti-fraud laws. Your organization has the right to defend its mark in court.

If you find that you are personally the victim of a phishing scam, then you should identify what information was compromised and then:

If the fraudster obtained your Bank Account, Credit, ATM or Debit Card information:

## Why Corporations Need to Worry About Phishing

Report the theft to your card issuer, and cancel the account

Check your statements for any unauthorized charges and follow up with your financial institution regarding their procedures for minimizing your liability to the charges

If the fraudster has obtained your personal identification information

Contact the credit reporting agencies:

Request that a fraud alert be placed on your record

Request a copy of your credit report and follow up on any unauthorized credit inquiries

Request that unauthorized credit inquiries be erased from your record

Notify your bank of potential fraud

File a police report with your local police department

File a report with the Social Security Administration

Notify the Department of Motor Vehicles and determine if an unauthorized driver's license number has been issued in your name

Notify the Federal Trade Commission ([www.ftc.gov](http://www.ftc.gov))

File a complaint with the Internet Fraud Complaint Center ([www.ifccfbi.gov/index.asp](http://www.ifccfbi.gov/index.asp))

Additional Internet Fraud Sites

CipherTrust is the leader in anti-spam and email security. Learn more by downloading our free whitepaper, "

" or by visiting

.

**Fishing for phishers.**

**By dDawg**

**Fishing for phishers. by dDawg**

Netcraft goes fishing for phishers.

Netcraft has released an Internet Explorer plug-in that could help people avoid becoming victims of online fraud.

The Internet security company heralded the plug-in toolbar, which displays information about the Web sites a surfer is visiting, as a strong weapon against phishing attacks.

The Netcraft Toolbar provides you with constantly updated information about the sites you visit as well as blocking dangerous sites, the company, best known for providing statistics on what software Web sites are running, stated in a posting. "This information will help you make an informed choice about the integrity of those sites."

The toolbar displays information about the popularity of a site, the country in which the site is hosted

## Why Corporations Need to Worry About Phishing

and the Internet address of the site. It also indicates whether other toolbar users have flagged the site as a possible phishing scam, which uses fake Web sites that look like they belong to a trusted provider, such as a bank, to fool people into handing over sensitive personal information.

The effectiveness of the toolbar will largely depend on how widely the software is adopted, Netcraft Director Mike Pettejohn said.

"If the big banks go for branded versions to give to their customers, then (it will be) very effective," he said. "It's only been public for two days, and there is already an effective community of people blocking phishing sites."

The software is available as a plug-in for Microsoft's Internet Explorer Web browser and can be downloaded from Netcraft. A version of the program that runs on the Firefox browser from the Mozilla Foundation is also under development, the company said.

An elite team of regular "Joes's" fighting back & making huge cash online one day at a time.

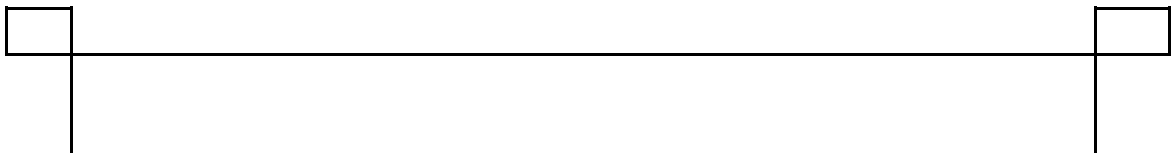
dDawg as a team has been able to create a profit on the internet.

<http://www.str8junk.com/heavyhitter.html>

An elite team of regular "Joes's" fighting back & making huge cash online one day at a time. dDawg as a team has been able to create a profit on the internet. <http://www.str8junk.com/heavyhitter.html>



**This Free E-Book has been brought to you by [Natural-Aging.com](http://Natural-Aging.com).**



**100% Effective Natural Hormone Treatment**  
**Menopause, Andropause And Other Hormone Imbalances**  
**Impair Healthy Healing In People Over The Age Of 30!**