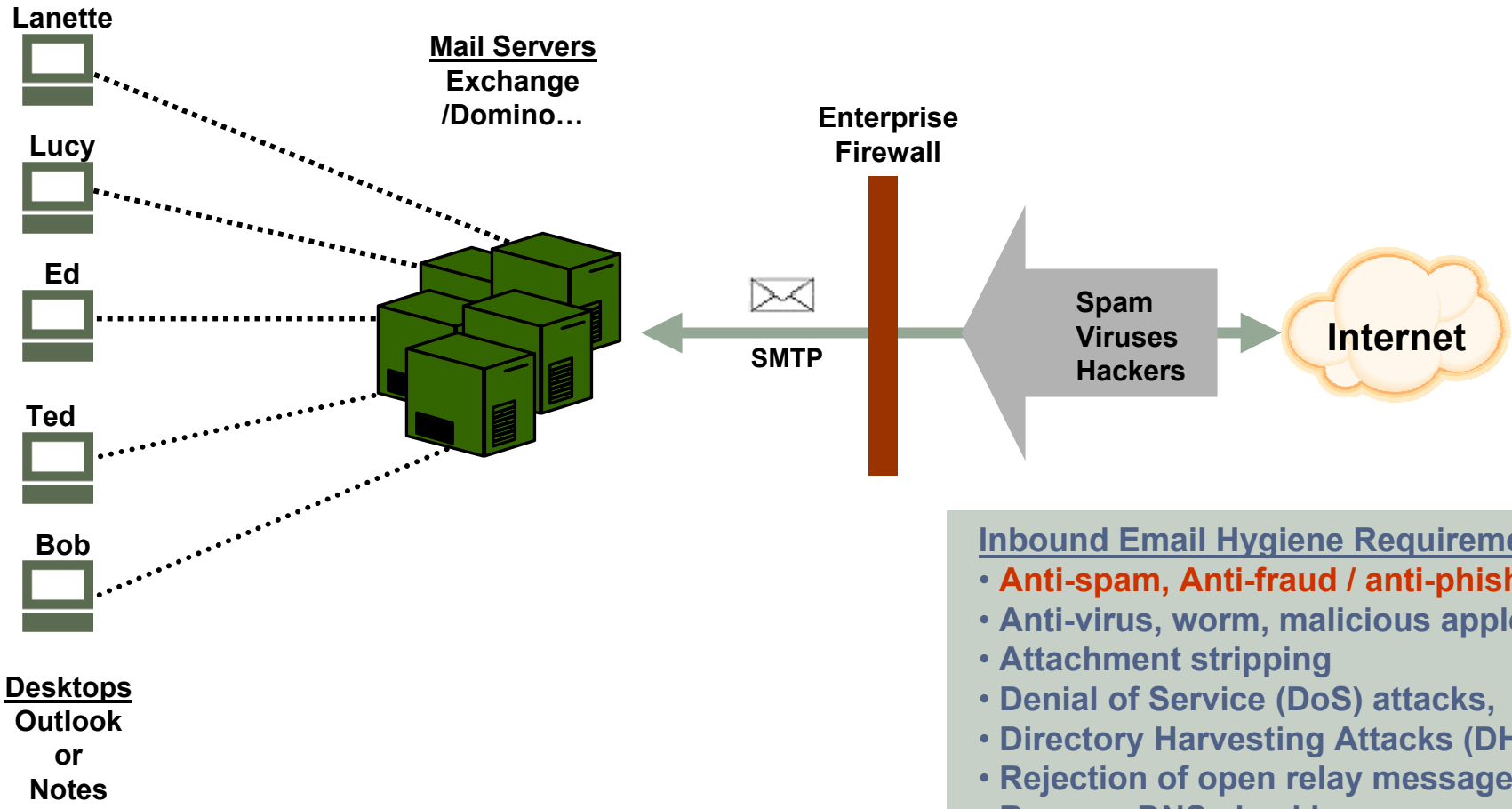
TUMBLEWEED COMMUNICATIONS

Tumbleweed® Email Firewall

Joe Fisher
Director of Product Management
February 17, 2004

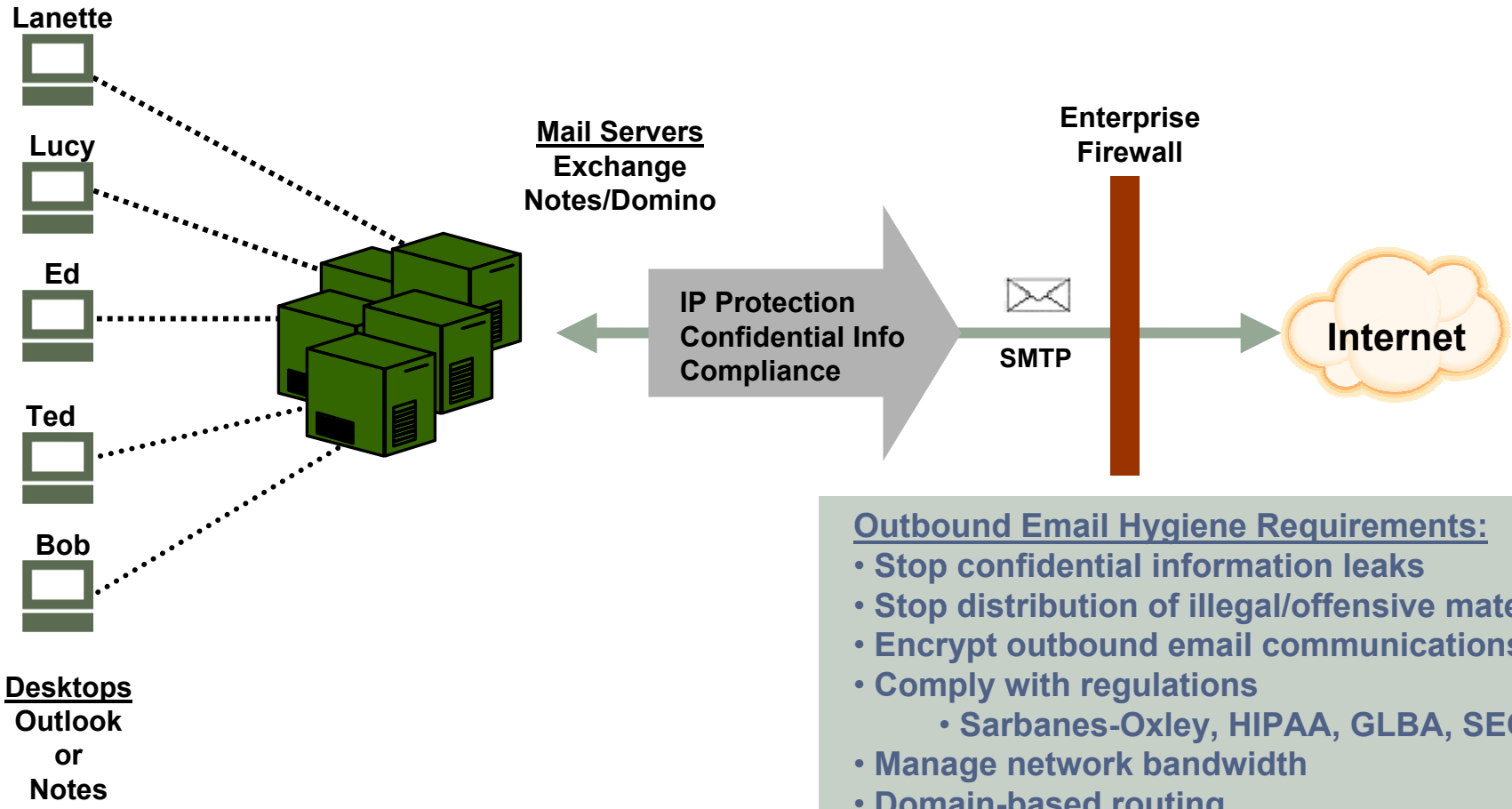
Inbound Email Threats



Inbound Email Hygiene Requirements:

- **Anti-spam, Anti-fraud / anti-phishing**
- Anti-virus, worm, malicious applets
- Attachment stripping
- Denial of Service (DoS) attacks,
- Directory Harvesting Attacks (DHA)
- Rejection of open relay messages
- Reverse DNS checking

Outbound Email Threats



Outbound Email Hygiene Requirements:

- Stop confidential information leaks
- Stop distribution of illegal/offensive material
- Encrypt outbound email communications
- Comply with regulations
  - Sarbanes-Oxley, HIPAA, GLBA, SEC…
- Manage network bandwidth
- Domain-based routing
- Address rewriting

Spam is the tip of the iceberg!

TUMBLEWEED COMMUNICATIONS

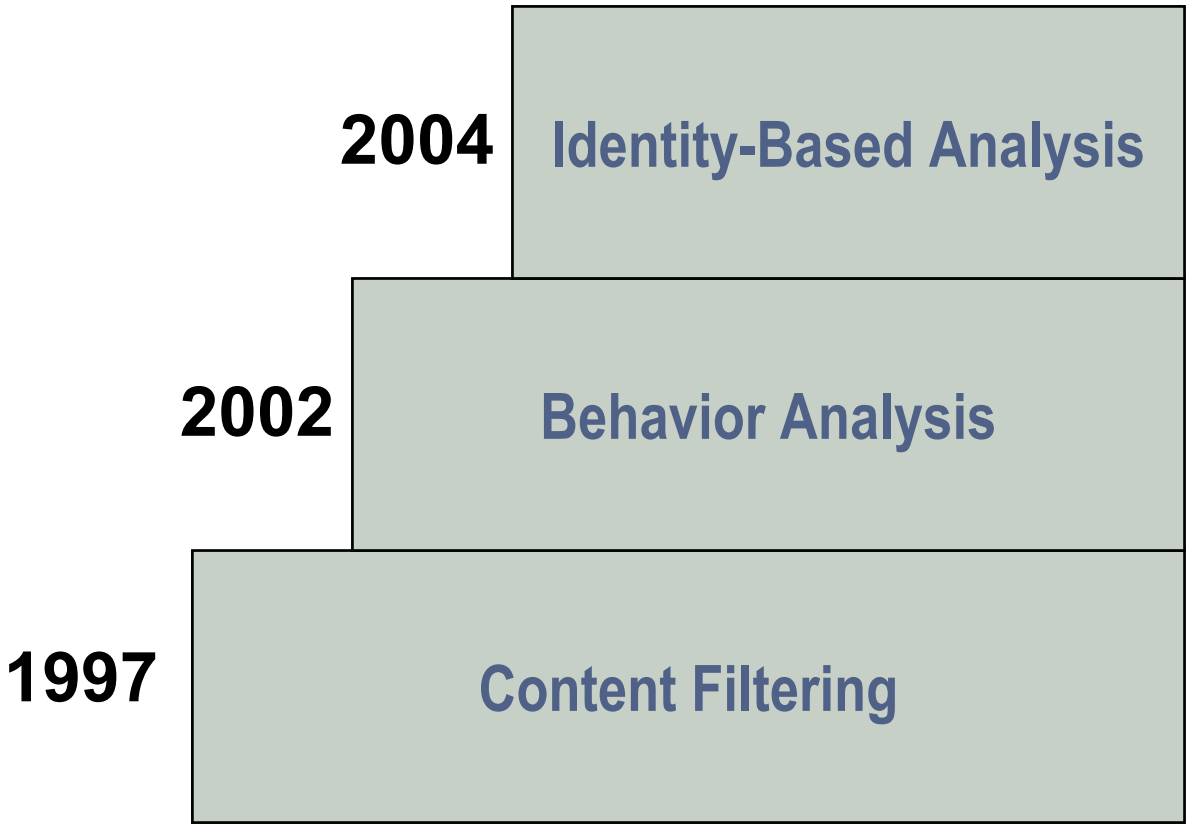
Phishing attacks!

- "Spoofed" email messages and websites designed to fool recipients into divulging personal financial information
- Sent via Spam techniques
- Operated by criminals, and getting harder to detect
- Customers lose privacy, money and/or services
  - » Estimates as high as 20% of targeted end-users fall for scams*

*Top 5 US Bank

Ultimately customers lose faith in the Internet as a means to conduct business because they can not determine who they can trust

Evolution of Anti-spam Technologies



- SPF, DomainKeys, etc
- Digital Signatures
- IP Whitelisting

- Heuristics
- Bayesian
- Statistical Analysis

- Lexical Analysis
- Weighted Word Lists
- Regular Expressions
- Signature/Hash

Tumbleweed's stance:"Cocktail" approach is the most effective.

Phishing Trends

TUMBLEWEED COMMUNICATIONS

- **Reported attacks**
  - Nov – 21 total, 0.7 per day
  - Dec – 116 total (452% growth), 3.7/day avg
  - Jan – 176 total (52% growth), 5.7/day avg
- **Total estimated phishing attack email volumes**
  - Jan – 1.76 Billion
- **Most targeted companies**
  - Unique attacks reported against 28 different companies in Jan
  - Ebay, Citibank, AOL are the top three

*Antiphishing.org

The Costs of Threats in the Enterprise

TUMBLEWEED COMMUNICATIONS

- **Reduced employee productivity**
  - Time spent deleting spam
  - Time spent retrieving false positives
- **Loss of valuable network resources**
  - Network storage and bandwidth
  - Mail server capacity
- **Reduced IT productivity**
  - Technical support
  - IT administration
- **Legal liability**
  - Risk of hostile workplace lawsuits
- **Phishing and Fraud**
  - Customers lose money, identity
  - Companies lose reputation/brand and customer trust

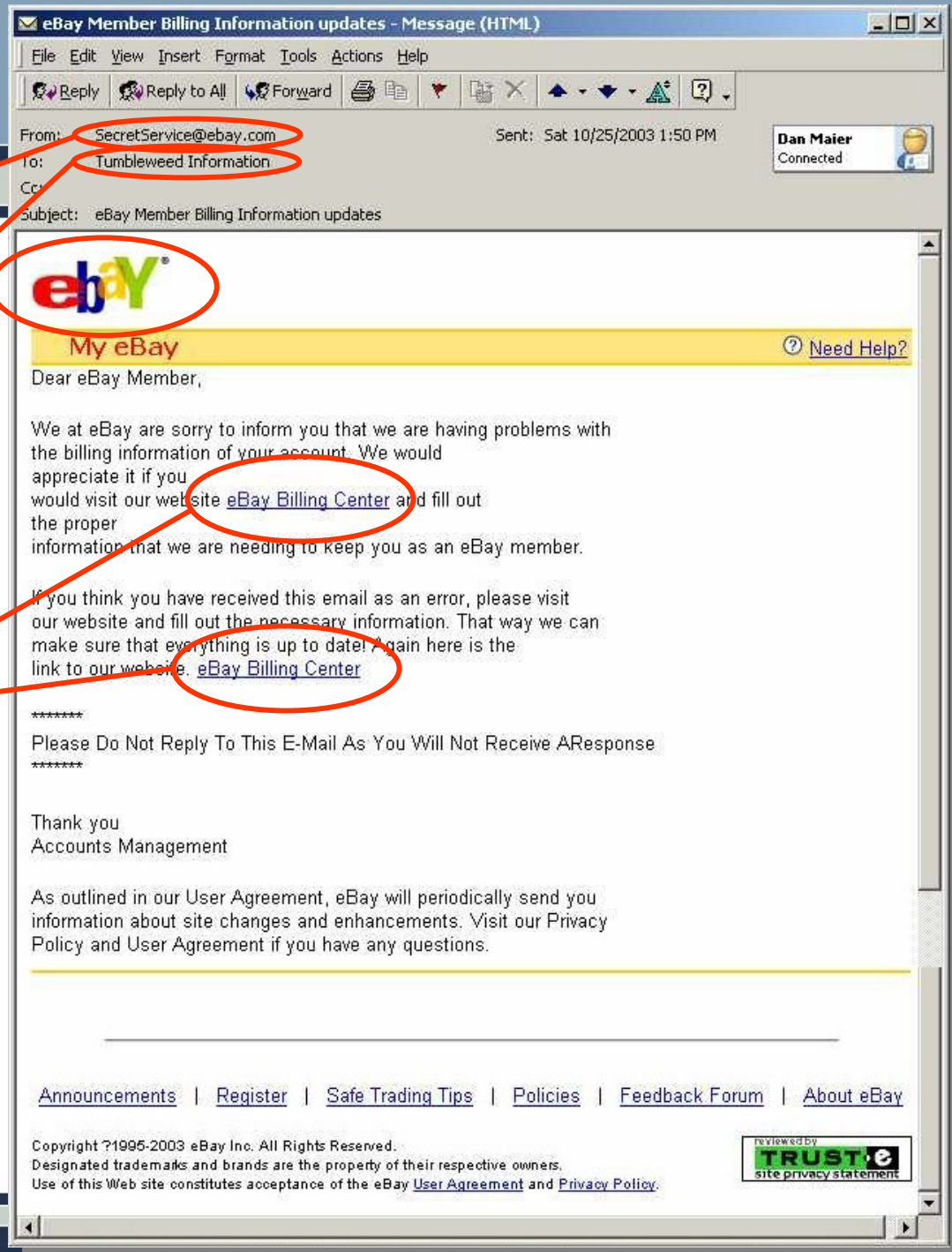
Phishing Attacks

Spoofed Email Address
(SecretService@ebay.com)

Spam Mass Mailing

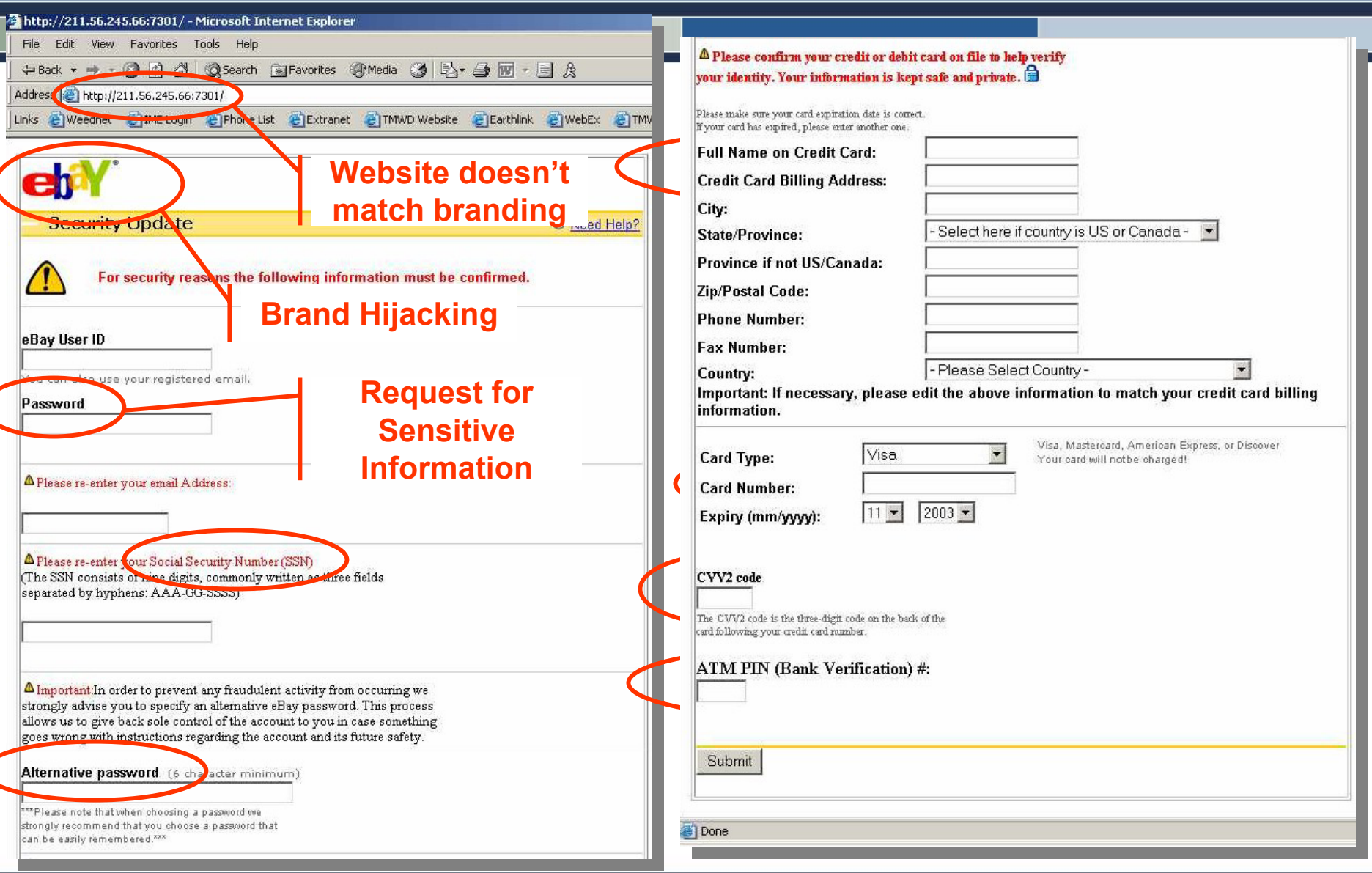
Brand Hijacking

Disguised Link to Phisher Site
href="http://www.ebay.com:tkbm6Yjkimgd234d
gdfhfnbjghuiiqrfgfdhgjgtWdfdbhjiuEbnkuod5fEtn
uo3243h*@211.56.245.66:7301/"



Phishing Attacks

TUMBLEWEED COMMUNICATIONS



Can You Detect It?

TUMBLEWEED COMMUNICATIONS

- **Website URL may not match hijacked company**
  - » phisher websites are increasingly hosted offshore, and may show a numeric IP address rather than a domain

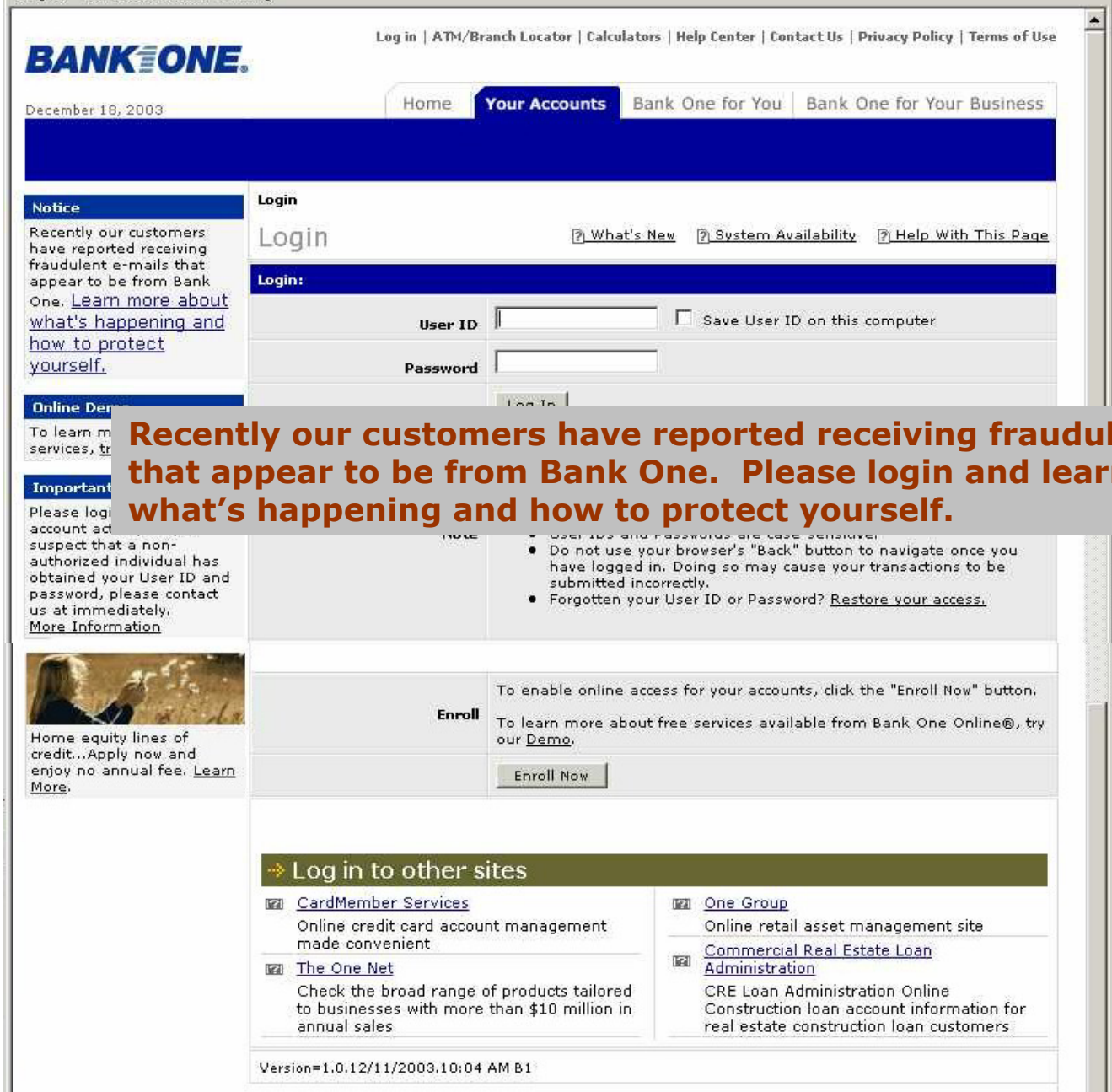
- **IE Bug lets phishers make fake URLs** 

  - » phishers are using an IE browser vulnerability that lets them mask the real site address with the hijacked company's website domain

- **Other devious ways to trick you**
  - » Popups and redirections

Ultimately customers lose faith in the Internet as a means to conduct business because they can not determine who they can trust

From: Bank One [customerservice@bankone.com] Sent: Thu 12/25/2003 11:11 AM
To:
Cc:
Subject: Bank One Customer Warning



Recently our customers have reported receiving fraudulent e-mails that appear to be from Bank One. Please login and learn more about what's happening and how to protect yourself.

From: Visa International Service <security@visa-security.com>
To: [redacted]@juno.com
Date: Tue, 23 Dec 2003 03:24:28 -0600
Subject: Visa Security Update
Message-ID: <AAA98SCTXAAARSDA@mx19.lax.untd.com>
Reply-To: Visa International Service <security@visa-security.com>
Received: from mx19.lax.untd.com (mx19.lax.untd.com [10.130.24.79])
by maildeliver05.lax.untd.com with SMTP id AAA98SCTXATPRVGA
for <[redacted]@juno.com> (sender <7869@mail.com>);
Tue, 23 Dec 2003 01:26:13 -0800 (PST)
Received: from 218.150.12.43 ([218.150.12.43])
by mx19.lax.untd.com with SMTP id AAA98SCTXAAARSDA
for <[redacted]@juno.com> (sender <7869@mail.com>);
Tue, 23 Dec 2003 01:26:12 -0800 (PST)
X-Mailer: Microsoft Outlook Express 6.00.2800.1158
MIME-Version: 1.0
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
X-MAIL-INFO:
437d5d893939455d38345d742538d1a92494b1c9357935a9f4fd2d89eda42d1ddd40f41d9485d5c4:
Organization: Visa International Service
X-ContentStamp: 2:3:1818088027
Return-Path: <7869@mail.com>
Message-ID: <AAA98SCTXAAARSDA@mx19.lax.untd.com>

Dear Customer,

Our latest security system will help you to avoid possible fraud actions and keep your investments in safety.

Due to technical security update you have to reactivate your account

Click on the link below to login to your updated Visa account.

To log into your account, please visit the Visa Website at

http://www.visa.com

We respect your time and business.
It's our pleasure to serve you.

Please don't reply to this email. This e-mail was generated by a mail handling system.

VISA

How Long To Take A Site Down?

TUMBLEWEED COMMUNICATIONS

- **Even once a phishing attack is detected, it takes an average of 160 hours to take it down.**
  - » It's in another country
  - » No cross-border Internet crime laws
  - » It may be running on a hacked server someplace

Billing Update Requested (URGENT) - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: AT&T Billing [billing@worldnet.att.net] Sent: Thu 1/8/2004 6:41 PM

To: [redacted]@worldnet.att.net

Cc:

Subject: Billing Update Requested (URGENT)

Recently we attempted to authorize payment from your credit card we have on file for you, but it was declined.

For security purposes, our system automatically removes credit card information from an account when there is a problem or the card expires.

Please resubmit the credit card, and provide us with new and complete information. To resubmit credit card information via our secure server, click the following link:

https://my.att.net/AuthN.login?sid=c0?p=addcreditcard

This is the quickest and easiest method of getting credit card information to us. Using the secure server will ensure that the credit card will be placed on account within 24 hours.

Member Services | HOME | MY AT&T | E-MAIL | FEATURES | SEARCH TOOLS | SHOP | HELP

Home / Help / Service Bulletins /

Have you found this Web site helpful? Let us know.

Notice to AT&T Internet Customers

You have been directed to this AT&T Web page as a result of having clicked a link within an e-mail you recently received. The e-mail likely appeared to have been sent by AT&T and requested that you either update your billing information or verify personal data associated with your current AT&T Internet account.

You may have received an e-mail message that appears to have been sent by AT&T. This e-mail directed you to click on a link to a Web site. This site would have asked you to provide personal information such as: driver's license, mother's maiden name, or your credit card account information.

AT&T has blocked access to the suspected fraudulent Web site and has diverted you to this notification page to protect you against possible credit card fraud and/or identity theft.

This e-mail message is unauthorized by AT&T and should be disregarded.

To facilitate our investigation into this incident, please forward the complete e-mail message you have received (with header information attached) to scam@abuse-att.net.

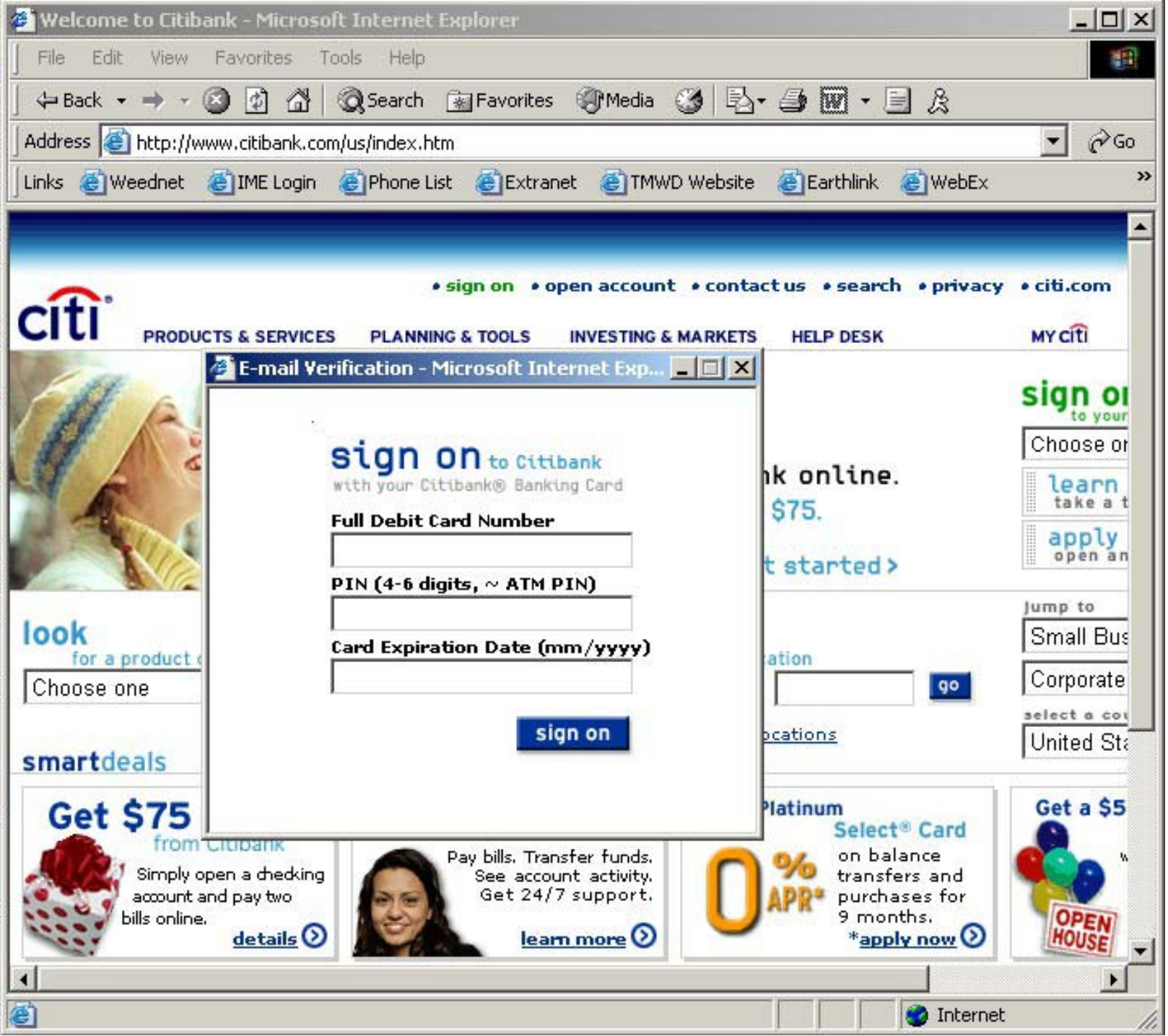
To obtain important information pertinent to protecting yourself against identity theft, you may wish to visit the US Federal Trade Commission's Identity Theft Web site, which is located at http://www.consumer.gov/idtheft/.

Average Losses?

TUMBLEWEED COMMUNICATIONS

- **It can cost $50k per phishing attack in administrative overhead***
  - » $50-60 per account
- **Phishers can net about $100k in financial theft per attack***
- **Up to 7 new attacks per day!**
- **Business and brand risk**

*Top 5 credit Card Issue


Welcome to Citibank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.citibank.com/us/index.htm
Go
Links Weednet IME Login Phone List Extranet TMWD Website Earthlink WebEx
citi
• sign on • open account • contact us • search • privacy • citi.com
PRODUCTS & SERVICES PLANNING & TOOLS INVESTING & MARKETS HELP DESK MY CITI
E-mail Verification - Microsoft Internet Exp...
sign on to Citibank
with your Citibank® Banking Card
Full Debit Card Number
PIN (4-6 digits, ~ ATM PIN)
Card Expiration Date (mm/yyyy)
sign on
look
for a product
Choose one
smartdeals
Get $75
from Citibank
Simply open a checking account and pay two bills online.
details
Pay bills. Transfer funds. See account activity. Get 24/7 support.
learn more
0% APR*
Platinum Select® Card
on balance transfers and purchases for 9 months.
*apply now
Get a $5
OPEN HOUSE
go
Jump to
Small Bus
Corporate
United Sta
Internet

How Can Phishing (Spam) Be Stopped?

TUMBLEWEED COMMUNICATIONS

1. Education
2. Detection
3. Prevention

Detection

TUMBLEWEED COMMUNICATIONS

- **"Domain name registration monitoring"**
  - Service to continuously monitor domain name registrars and the domain name system for domain names that infringe on a company's trademarked names, and could be used to launch spoofed websites to fool customers.

- **"Central Clearinghouse"**
  - Create a central clearinghouse of known phishing attacks shared all companies (banks, ISPs, technology vendors, law enforcement…)

Detection

TUMBLEWEED COMMUNICATIONS

- **"Spam Scanning"**
  - » There are a number of anti-spam vendors offering services to scan email in the wild and notify customers if they detect phishing attacks against that company.

- **"Spam Filtering“**
  - » There are many anti-spam vendors who are adding identified phishing attacks to their spam filters, to prevent it from getting to the desktop.

Prevention

TUMBLEWEED COMMUNICATIONS

- **"Strong Website Client Authentication"**
  - » Strongly authenticate any users visiting a business web site using two-factor authentication
- **"Mail Server Authentication"**
  - » Stop spoofing using enhanced DNS capabilities to verify the IP address of a sender's email server
- **"Mail Sender Authentication via Digital Signatures"**
  - Use S/MIME/PGP/etc digital signatures to sign outbound mail - provide signature verification at the gateway

Conclusion

TUMBLEWEED COMMUNICATIONS

- **Industry/market direction:**

“Spam Filter Today,

Authenticated Email Tomorrow”