Accountability
The key to defeating Internet Crime

Phillip Hallam-Baker
Principal Scientist
VeriSign Inc.

©2004 VeriSign Inc.

If cars were like computers…

VeriSign

…but

VeriSign

Cars are not designed for speed, cost or mpg.

VeriSign

Cars

Safety

Reliability

Luxury

VeriSign

The luxury computer has not yet been made

VeriSign

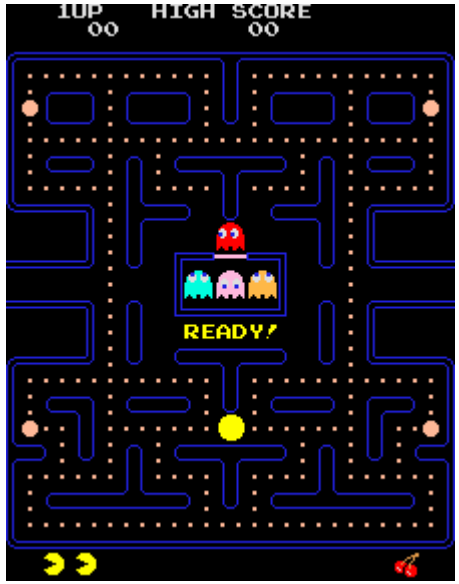
Computers

Pig to use

Break every hour

Steal your life savings

VeriSign



But luxury is not impossible

VeriSign

Making driving safe

VeriSign

Accountability

VeriSign

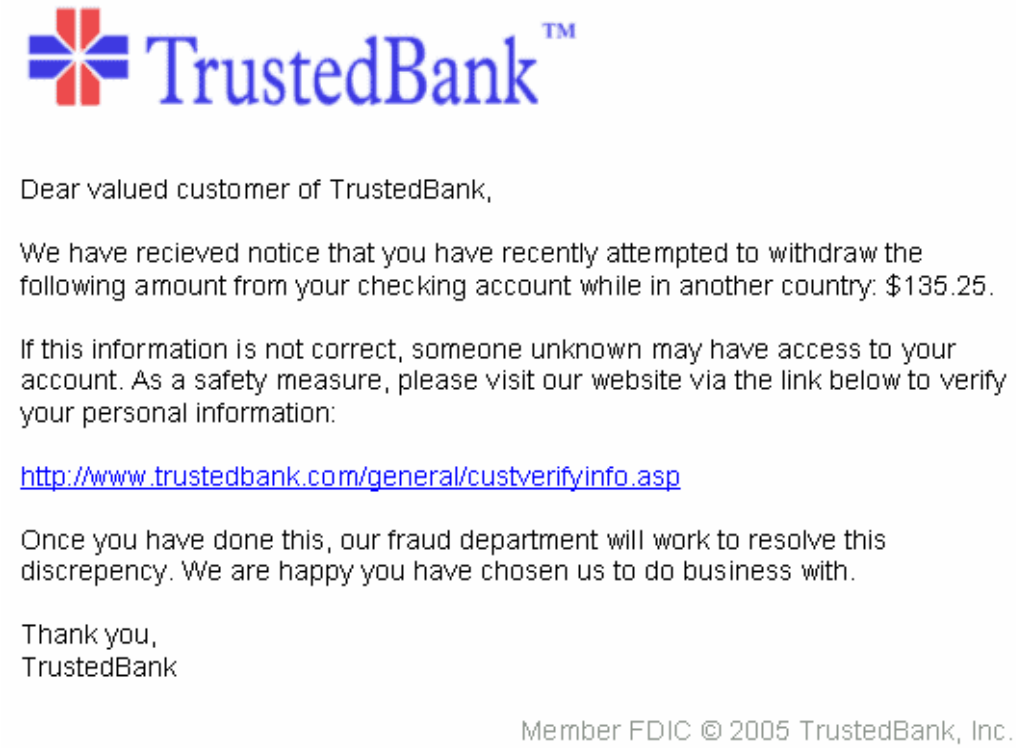
How do we use Accountability to stop Internet Crime?

VeriSign

Professional Internet Crime

VeriSign

Phishing



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

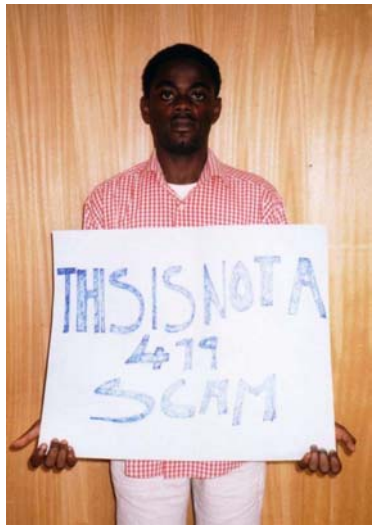
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

VeriSign

Extortion

VeriSign



419eater.com

Advance Fee Frauds

VeriSign

What is to be done?

VeriSign

User Education

(Blame the User)

VeriSign

The Law

Trigger Penalties

Tripwire Offenses

VeriSign

Change the Internet

Make the Internet Infrastructure crime resistant

VeriSign

Wasn’t that the plan?

VeriSign

Permission Based Security

Access Control:

Confidentiality

Integrity

VeriSign

Accountability Based Security

Authentication

Accreditation

Consequences

VeriSign

Accountability Based Security

Authentication

Accreditation

Consequences

VeriSign

How do we apply accountability?

VeriSign

What is Phishing?

Credential theft

Impersonation of a trusted brand

VeriSign

Stopping Phishing

VeriSign

Tactical:
Stop Attacks in Progress

VeriSign

VeriSign's Anti-Phishing Solution

- + Policy, Programs & Education
- + 2-Factor Authentication
- + Fraud Detection
- + Tokens

- + Brand Management
- + Domain Name Monitoring
- + Web Crawlers
- + Spam Filters
- + Customer Notification

- + 24x7 Support
- + Integrated Processes
- + Global Abuse Contact DB
- + Shutdown Phishing Sites
- + Damage Assessment

- + Cyber Forensics
- + Subpoenas
- + Follow-up Investigation

- + Initial Incident Validations
- + Progress Reports
- + Investigative Report
- + Trend Reporting

VeriSign

Tactical:
A car alarm

VeriSign

How do we *stop* Phishing

VeriSign

What is Phishing?

Credential theft

Impersonation of a trusted brand

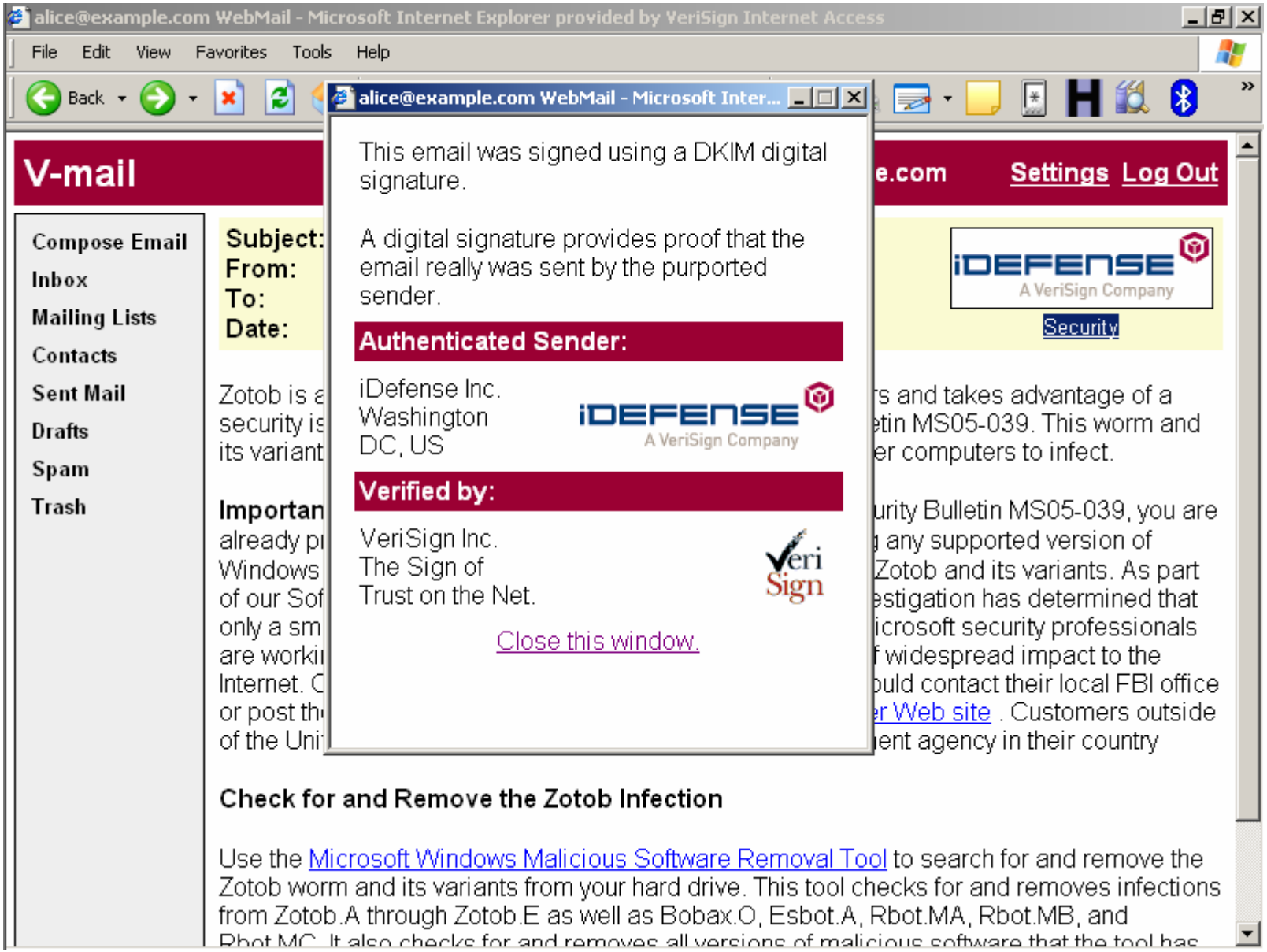
VeriSign

Strategic:
Theft proof Credentials

VeriSign

Strategic:
Theft proof Brands

VeriSign


alice@example.com WebMail - Microsoft Internet Explorer provided by VeriSign Internet Access
File Edit View Favorites Tools Help
Back
alice@example.com WebMail - Microsoft Inter...
This email was signed using a DKIM digital signature.
A digital signature provides proof that the email really was sent by the purported sender.
Authenticated Sender:
iDefense Inc.
Washington
DC, US
iDEFENSE
A VeriSign Company
Verified by:
VeriSign Inc.
The Sign of
Trust on the Net.
VeriSign
Close this window.
V-mail
e.com
Settings Log Out
Compose Email
Inbox
Mailing Lists
Contacts
Sent Mail
Drafts
Spam
Trash
Subject:
From:
To:
Date:
iDEFENSE
A VeriSign Company
Security
Zotob is a
security is
its variant
s and takes advantage of a
tin MS05-039. This worm and
er computers to infect.
Importan
already pr
Windows
of our Sof
only a sm
are worki
Internet. C
or post th
of the Uni
urity Bulletin MS05-039, you are
any supported version of
Zotob and its variants. As part
estigation has determined that
icrosoft security professionals
f widespread impact to the
ould contact their local FBI office
r Web site . Customers outside
ent agency in their country
Check for and Remove the Zotob Infection
Use the Microsoft Windows Malicious Software Removal Tool to search for and remove the Zotob worm and its variants from your hard drive. This tool checks for and removes infections from Zotob.A through Zotob.E as well as Bobax.O, Esbot.A, Rbot.MA, Rbot.MB, and

VeriSign

Secure Internet Letterhead

Every Web Site

Every Email Message

Every Instant Message

Every Voice or Video Call

VeriSign

How?

VeriSign

Technical Details

Open Standards

X,509 Certificate (ISO)

Domain Keys Identified Mail (IETF, in progress)

PKIX Logo Type Extension (IETF)

High Assurance Certificates (CA Forum)

VeriSign

Accountability

Brand owner is accountable to consumer

VeriSign

Accountability

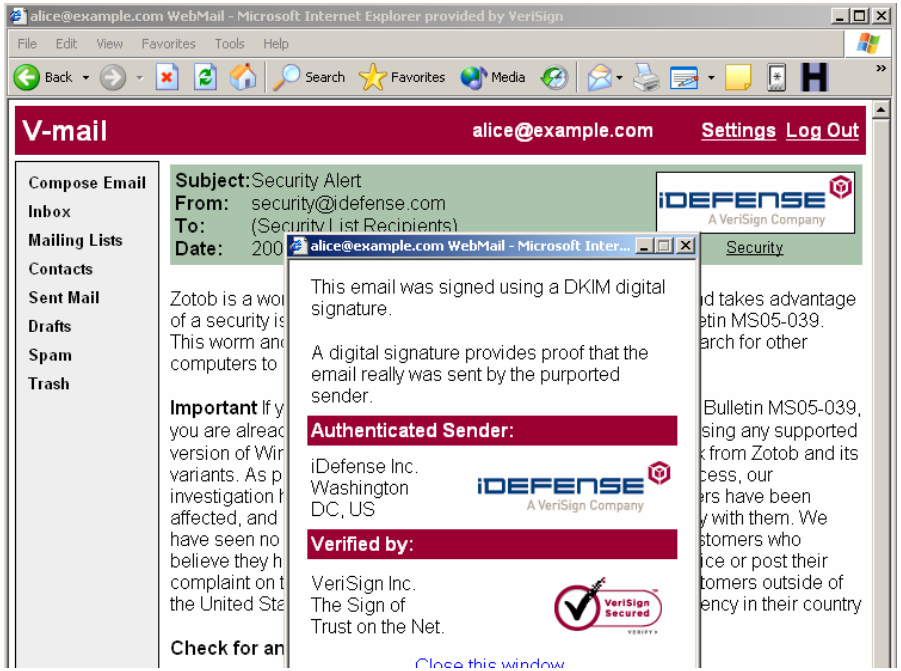
What if the certificate is issued to an attacker?

VeriSign

Who Guards the Guardians?

Accountability

VeriSign



Accountability

Our brand on the line

VeriSign

How to stop spam

Accountability

VeriSign

Accountability

Who sent the email?

Are they likely to be a spammer?

Consequences for default

VeriSign

Strategic:
Theft proof Credentials

VeriSign

oath

Theft-proof Credentials

VeriSign

But how to deploy?

VeriSign

Keyboards with card readers?

VeriSign

Open Standards
for Tokens

VeriSign

Open Standards for Interconnect

VeriSign

Identity 2.0

VeriSign

A Pain Point, not a technology

VeriSign

Blogs

VeriSign

Single Sign on
(for consumers)

VeriSign

Work in progress

SAML, WS-Security, DIX, XKMS, LID, OpenID, LID, HTTP-Auth…

(we can work it out)

VeriSign

What must be

VeriSign

Consumer can control their own security

I can buy a bike lock at a store,

I need an Internet lock more

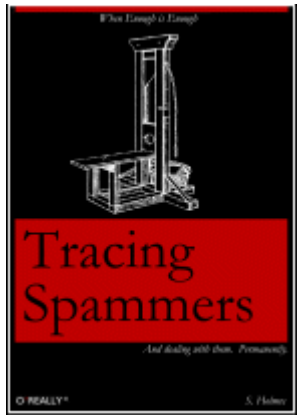
VeriSign

Authentication

VeriSign

Accreditation

VeriSign



Consequences

VeriSign

Accountability

VeriSign

Thank You

Questions

VeriSign