



Accountability

The key to defeating Internet Crime

Phillip Hallam-Baker

Principal Scientist
VeriSign Inc.



If cars were like
computers...

...but

Cars are not designed for
speed, cost or mpg.

Cars

Safety

Reliability

Luxury



The luxury computer has
not yet been made

Computers

Pig to use

Break every hour

Steal your life savings



But luxury is not impossible



Making driving safe

Accountability

How do we use
Accountability to stop
Internet Crime?



Professional Internet Crime

Phishing



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.

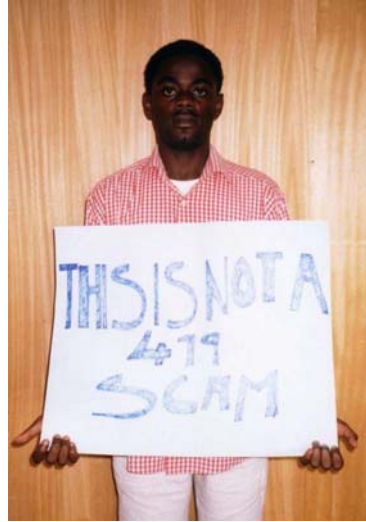
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.





Extortion



419eater.com

Advance Fee Frauds

What is to be done?

User Education

(Blame the User)



The Law
Trigger Penalties
Tripwire Offenses

Change the Internet

Make the Internet Infrastructure crime resistant



Wasn't that the plan?

Permission Based Security

Access Control:
Confidentiality
Integrity

Accountability Based Security

Authentication
Accreditation
Consequences

Accountability Based Security

Authentication

Accreditation

Consequences

How do we apply
accountability?

What is Phishing?

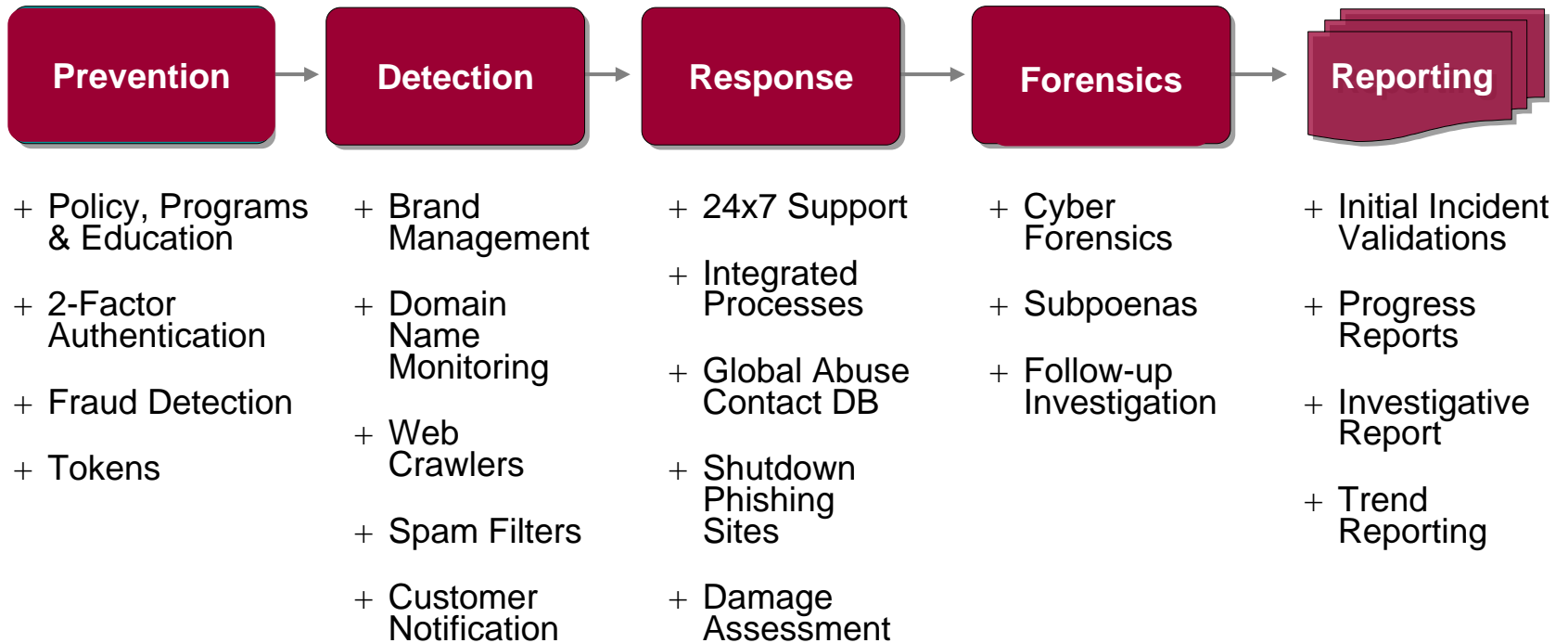
Credential theft

Impersonation of a trusted brand

Stopping Phishing

Tactical: Stop Attacks in Progress

VeriSign's Anti-Phishing Solution



Tactical: A car alarm

How do we stop Phishing

What is Phishing?

Credential theft

Impersonation of a trusted brand

Strategic: Theft proof Credentials

Strategic: Theft proof Brands

alice@example.com WebMail - Microsoft Internet Explorer provided by VeriSign Internet Access

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Bluetooth

V-mail


- Compose Email
- Inbox
- Mailing Lists
- Contacts
- Sent Mail
- Drafts
- Spam
- Trash

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




Verified by:

VeriSign Inc.
The Sign of Trust on the Net.



[Close this window.](#)

alice@example.com [Settings](#) [Log Out](#)



[Security](#)

Important

Zotob is a security is its variant already p Windows of our Sof only a sm are worki Internet. C or post th of the Uni

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 Rbot.MC. It also checks for and removes all versions of malicious software that the tool has

and takes advantage of a etin MS05-039. This worm and er computers to infect.

curity Bulletin MS05-039, you are g 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 [er Web site](#) . Customers outside ent agency in their country



Secure Internet Letterhead

Every Web Site



Every Email Message



Every Instant Message



Every Voice or Video Call



How?

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)

Accountability

Brand owner is accountable to consumer

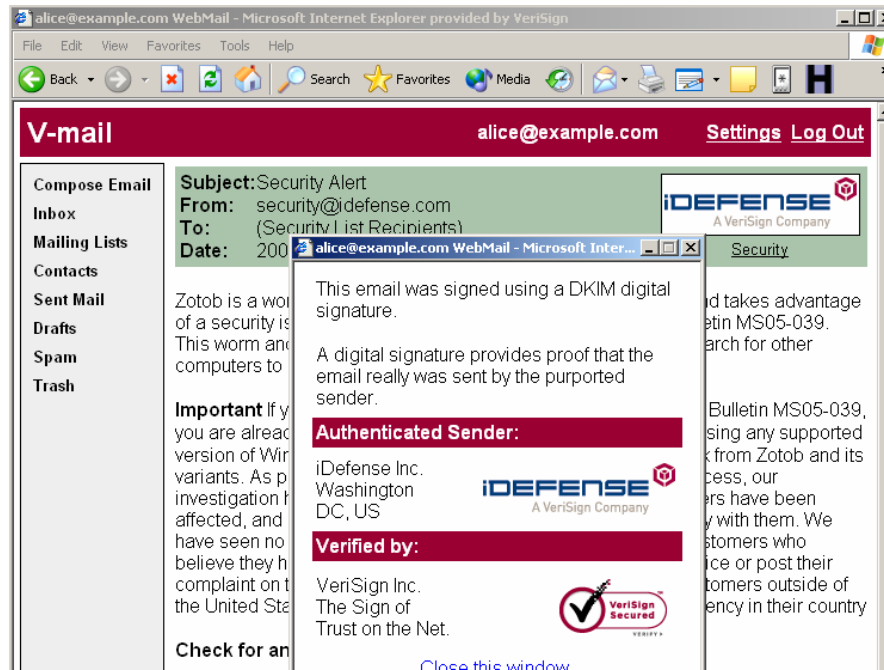
Accountability

What if the certificate is issued to an attacker?



Who Guards the Guardians?

Accountability



Accountability

Our brand on the line



How to stop spam

Accountability

Accountability

Who sent the email?

Are they likely to be a spammer?

Consequences for default

Strategic: Theft proof Credentials



oath

Theft-proof Credentials

But how to deploy?

Keyboards with card
readers?

Open Standards for Tokens





Open Standards for Interconnect

Identity 2.0

A Pain Point, not a
technology

Blogs

Single Sign on (for consumers)

Work in progress

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

(we can work it out)

What must be

Consumer can control their own security

I can buy a bike lock at a store,
I need an Internet lock more



Authentication



Accreditation



Consequences

Accountability

Thank You

Questions

