INTERNET CITIZENS BEWARE! YOU'RE BEING PHISHED!

This is totally phreaking me out!

"PHISHING" IS AN EMAIL SCAM WHERE SOMEONE IS "FISHING" FOR FINANCIAL INFORMATION.

What the heck! Here's my account number and PIN!

IT DOES IT BY MIMICING THE LOOK OF A LEGITIMATE COMPANY'S WEB SITE.

Ooo. I've got e-mail on penis enlargement and an urgent message from my BANK.
Fighting Phishing Attacks
Lightweight Signatures for Email

Ben Adida
ben@mit.edu
MIT Computer Science and Artificial Intelligence Lab

CRCS
November 2nd, 2005
(joint with David Chau, Susan Hohenberger and Ronald L. Rivest)
This Talk

- The evolution of phishing
- The email authentication problem
- Building an email authentication architecture
- Privacy concerns
From: eBay Billing Department <Billing@eBay.com>
Subject: Credit/Debit Update
Date: April 8, 2005 6:48:27 PM EDT
To: Ben Adida (E-mail)

Dear eBay member,

We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our eBay Billing Center and fill out the proper information that we are needing to keep you as an eBay member. If you don't comply until the 15 April 2005, your eBay membership may be suspended, or even deleted.

Click here to complete our web form.

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Thank you!
My eBay

New to eBay?

If you want to sign in, you'll need to register first.

Registration is fast and free.

Register >

or

Already an eBay user?

View all your bidding and selling activities in one location.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

Sign In Securely >

Keep me signed in on this computer unless I sign out.

Account protection tips
Be sure the Web site address you see above starts with https://signin.ebay.com/

Microsoft Passport users click here.
One in 20 'fall for online fraud'

One in 20 UK internet users say they have lost money through online scams, research into spam emails suggests.

Almost half say they have received so-called phishing emails aimed at tricking them into revealing details like online banking passwords.
this review is gathering information from community members on their usage of and satisfaction with medical care at MIT, and the Task Force has constructed a survey for students to provide their feedback.

Your time is valuable, especially at this busy time of year, but I hope that you might be willing to take about fifteen minutes to complete a web-based questionnaire. Your participation is entirely voluntary, and you may answer as few or as many questions as you wish. Your response will be treated as confidential, and data gathered will be reported in summary format. I urge you to be as candid as possible in your answers, as this is a very important issue for you and for the students who will follow you at MIT.

You may enter the survey from <http://web.mit.edu/surveys/medical/>. This survey authentication requires a current MIT certificate.

If you have any questions, please send them to med-survey@mit.edu.

Sincerely,
Susan Hockfield
Beware: E-Mailed Surveys May Involve 'Phishing'
Scammers Seek Bank Account Numbers

By Audrey Laganas
From: Burgess-Gregg, Mary
Sent: Thursday, December 02, 2023
Subject: Presidential Recognition

I am pleased to inform you that I am more specific at this point be candidates.

I am contacting you now because we need to request a name check from the FBI, as we do with all persons being considered for Presidential recognition. In light of procedures put in place by the White House Counsel's Office, we must receive your written consent prior to requesting the name check. The request a name check from the FBI, 

http://ostp.gov/FBInamecheck.pdf

form should be faxed immediately,

NEOB
(202) 456-6130
(202) 456-6027 (fax)
MBurgess-Gregg@ostp.eop.gov
Fax Attack

New scam asks people to fax away data
Published: August 11, 2005, 7:48 AM PDT

By Dawn Kawamoto
Staff Writer, CNET News.com

Phishers have added a new lure to their tackle boxes: e-mails that ask people to fax sensitive information to bogus security investigators.
We cannot trust email

• “Never click on a link provided in an email asking for personal information.”
  American Banking Association (Dec. 2004)

• “Do be wary of clicking on links in e-mail messages.”
  Microsoft (Feb. 2005)

• “Don't automatically assume that any e-mail is from the ‘From’ address.”
  Bruce Schneier (Dec. 2004)
“Fear of phishing corrodes trust [...] in email as a vehicle”

“Don't click on links in emails from financial institutions and other organizations that have your personal information”

“Don't trust phone numbers in emails. These can be faked, too.”

“We hate to say that, because such email communications are supposed to make life easier.”
New type of phishing could hit mobile phone users

René Millman 1 Nov 2005 13:13

Experts have warned of a new type of phishing that could siphon bank details from mobile phone users.

Mophophishing is where hackers send
Phishing reveals a serious problem with email

We need to fix the email platform
SMTP Today

**DNS**
- foo.com
- MX Record: mail.foo.com

**E-mail Flow**
1. Alice
2. MX: mail.foo.com
3. E-mail sent to mail.foo.com
4. E-mail received by Bob
No Proof of Origin

Alice

wonderland.com
outgoing
mail server

?  

phish.com

mail.foo.com
incoming
mail server

Bob
Many Proposals

• Web-based solutions:
  checking links, better passwords, DSS,...

• Spam-like filtering
  identify bad emails by content

• Sender ID / Sender Policy Framework
  declaring authorized outgoing mail servers

• DomainKeys
  outgoing mail server signs all emails
A Platform of Trust

We want to provide Just Enough Trust
### Raising the Bar

<table>
<thead>
<tr>
<th>Spoof Outgoing</th>
<th>Intercept Incoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect to port 25 of Bob’s mail server, send data.</td>
<td>crack Bob’s IMAP/POP authentication or sniff Bob’s network consistently</td>
</tr>
</tbody>
</table>

**Diagram:**
- **Alice**
- **Bob**

**Steps:**
1. Alice spoofs outgoing connections to Bob's mail server.
2. Alice sends data to Bob.
3. Alice intercepts incoming communications to Bob.
4. Alice cracks Bob's IMAP/POP authentication or sniffs Bob's network consistently.
Building Lightweight Signatures
Basic Signatures

\[
sign_{\text{wonderland}}(PK_{\text{alice}}, \text{“alice@wonderland.com”})
\]
DNS to distribute Domain-Level Keys

[DomainKeys]
Email Authentication

Scenario

Alice
alice@wonderland.com

Bob
bob@foo.com

Authority

wonderland

SK_{wonderland}

PK_{alice}

SK_{alice}

From: Alice
To: Bob
Subject: CRCS Seminars

The CRCS Seminars are awesome! I love those bagel and lox sandwiches. You should come.

Thinking of you,
Alice

sign_{alice}(message)

PK_{alice}

sign_{wonderland}(PK_{alice}, "alice@wonderland.com")
Email Authentication

- certifying a user’s public key can add significant overhead.
- distributing the secret key to all user access points is tricky.

... unless we rethink the security requirements a bit.
Email-Based Authentication

[Gar2003]
Server-Managed User Keys

Scenario

Alice
alice@wonderland.com

Authority

wonderland

$SK_{\text{wonderland}}$
$PK_{\text{wonderland}}$

DNS

wonderland.com

From: Alice
To: Bob
Subject: CRCS Seminars

The CRCS Seminars are awesome! I love those bagel and lox sandwiches. You should come.

Thinking of you,
Alice

$s_{\text{signature}}(\text{message})$

$PK_{\text{alice}}$

signwonderland($PK_{\text{alice}}$, “alice@wonderland.com”)
From: Alice
To: Bob
Subject: CRCS Seminars

The CRCS Seminars are awesome! I love those bagel and lox sandwiches. You should come.

Thinking of you,
Alice

From: Alice
To: Bob
Subject: CRCS Seminars

The CRCS Seminars are awesome! I love those bagel and lox sandwiches. You should come.

Thinking of you,
Alice
DomainKeys

- intra-domain authentication?
- SK must be online
- mail-forwarding services?

... can we do better?

Alice
alice@wonderland.com

Authority
wonderland
$SK_{wonderland}$

From: Alice
To: Bob
Subject: CRCS Seminars
The CRCS Seminars are awesome! I love those bagel and lox sandwiches. You should come.
Thinking of you,
Alice

alice@wonderland.com
Can we get the benefits of both user keys and domain keys?
ID-Based Crypto

"bob@foo.com"

keyserver

MSK

MPK

PK_{bob}

SK_{bob}

Alice

Bob
ID-based Domains

$MPK_{\text{wonderland.com}}$

$SK_{\text{alice@wonderland.com}}$

$MSK_{\text{wonderland.com}}$

$MPK_{\text{foo.com}}$

$SK_{\text{bob@foo.com}}$

$MSK_{\text{foo.com}}$

Alice

Bob
DNS to distribute Master Public Keys

DNS

wonderland.com

foo.com

MPK_wonderland.com

MPK_foo.com

Publish

wonderland.com
key server

MSK_wonderland.com
Email-Based Authentication for User Secret Keys

Alice

wonderland.com
incoming
mail server

wonderland.com
keyserver

$MSK_{\text{wonderland.com}}$

$SK_{\text{alice@wonderland.com}}$

Alice
Lightweight Signatures

1. PUBLISH

From: Alice
To: Bob
Subject: CRCS!
Salil is the man.
Signed: Alice

2. "alice@wonderland.com"

3. MPK_{wonderland}

4. MPK_{wonderland}

5. MPK_{wonderland}

6. Bob

Peter Pan (Network)

Our Scenario
Realistic Deployment

• **Incremental Protection**
  Each domain can implement Lightweight Sigs when it wants to protect its users from spoofing.

• **Minimized User Intervention**
  With domain policies, there is no grey area: emails are either good or bad and require no user judgment.
Deployment Flexibility

• Upgrade the Mail Client & Deploy an Internal Keyserver
  ➔ mail client performs sign & verify
  ➔ keyserver distributes user secret keys

• Upgrade the Mail Server
  ➔ sign at outgoing mail server
  ➔ verify at incoming mail server
Origin of Lightweight Sigs

- Classic PGP or S/MIME
  - Domain-Managed User Keys
  - Domain-Level Key

Lightweight Signatures
Privacy Concern!

Every email is now publicly verifiable.
So What?

- Alice likes Bob
- Eve likes Bob
- Bob likes to gloat.

What if Bob publishes Alice’s Email on his blog?

This changes the nature of email.

Alice’s Email - August 30th, 2005
Check out what Alice wrote me earlier today! Crazy stuff.... who knew?
Hey Bob,

Wanna meet for coffee? I'd love to get to know you better.

Signed:
Alice or Bob
Identity-Based Sigs, again

- Public Keys are available **before** user has generated them.
- Public Keys are available using only the domain-based master public key in the DNS.
- If a domain has an MPK, then it can be used for repudiation
- If a domain doesn’t have an MPK, then a public repudiation service can be used instead.
Research Papers

• ACHR2005
  Lightweight Signatures for Email

• AHR2005
  Ad-Hoc Group Signatures from Hijacked Keypairs
Implementation

- Working prototype using a web-based key distribution, simple DNS server, and Emacs Rmail client.
- More involved usability study in the next few months, multiple domains, real mail client.
- Talk to us if you’re interested.
Summary

- Phishing reveals an email trust problem
- Lightweight Signatures can do everything DomainKeys can do.... and more
  - end-to-end support of all email apps
  - client-side or server-side computation
- Don’t forget about privacy!
Questions?
Some Crypto

Basic RSA

\[ PK = (n, e); \quad n = pq \quad SK = d \]

\[ \text{Enc}(m) = m^e \mod n \]

\[ \text{Dec}(c) = c^d \mod n \]

GQ ID-based Signatures

\[ MPK = (n, e) \]

\[ MSK = d \]

\[ PK_{ID} = H(ID) \in Z^*_n \]

\[ SK_{ID} = H(ID)^d \in Z^*_n \]

\[ s_1 = r^e \]

\[ \alpha = H(r^e, m) \]

\[ s_2 = r^{SK\alpha} \]

\[ s_2^e = s_1^{PK\alpha} \]