

Phishing Attempts - Determine what is legitimate and what is fraud

Dan Armstrong, Director – Technical Support Services, Plano Independent School District

Dan Armstrong has worked with the Plano Independent School District for 17 years in the technology department. He began in the Networking department as an engineer and has seen the district grow from multiple independent networks to an enterprise system with over 34,000 computers. As the Director, his responsibilities also include all voice, video and data services that run on a private fiber network that spans over eighty miles and connects over seventy locations.

■ *Did You Know...*

The word phishing comes from the analogy that Internet scammers are using e-mail lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting users. Since hackers have a tendency to replacing "f" with "ph" the term phishing was derived.

What is Phishing?

- (fish'ing) (n) The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a web site where they are asked to update personal information such as passwords, credit card, social security and bank account numbers, that the legitimate organization already has. The web site, however is bogus and set up only to steal the user's information.

Webopedia definition

Phishing Techniques

- Official looking and sounding emails
- Copies of legitimate corporate emails with minor URL changes
- Standard virus/worm attachments to emails
- Fake postings to popular message boards and mailing lists
- Use of fake Mail From: addresses
- IP addresses instead of domain names in hyperlinks that address the fake web site
- Registering similar sounding DNS domains and setting up fake web sites that closely mimic the domain name of the target web site.
- Embedding hyperlinks from the real target web site into the HTML content of an email about the fake phishing web site.
- Encoding or obfuscating the fake web site URL.
- Configuring the fake phishing web site to record any input data that the user submits, silently logs them and then forwards the user to the real web site.
- Setting up a fake web site to act as a proxy for the real web site of the target brand.
- Using malware to manipulate the hosts file on a victim's PC

Tips to help you recognize phishing scams and fraudulent email

- Key phrases
- Generic greeting
- Forged link-beware of the @ symbol in the URL
- Insecure site-look for https://
- Requests personal information
- Sense of urgency
- Spelling errors
- Poor grammar
- Warns that you've been a victim of fraud

>>>

From: "Bank Of America" <Service@bankofamerica.com>

To:

Date: 3/29/2008 7:22 AM

Subject: Your Online Banking is Locked

Your Online Banking is Locked

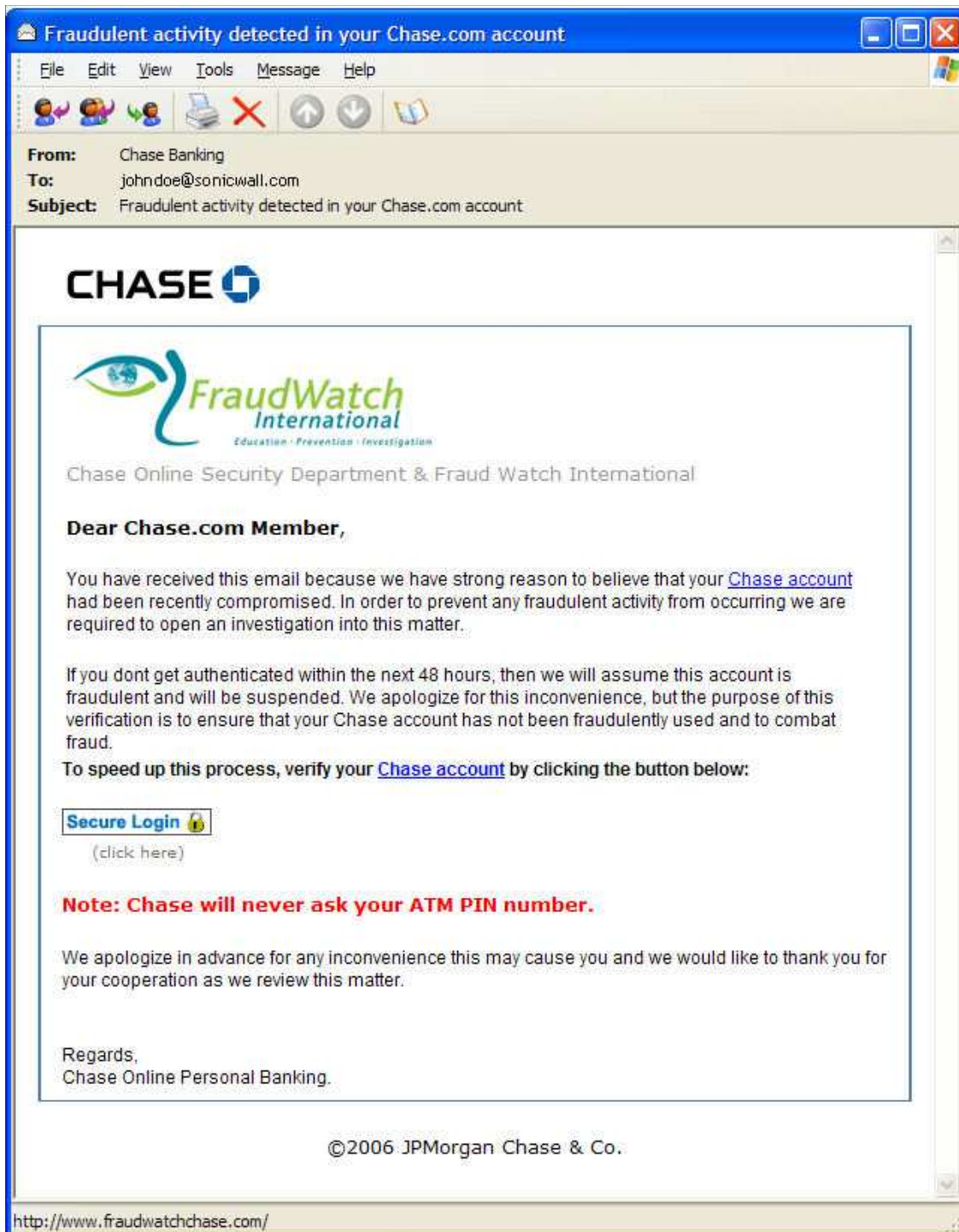
We recently reviewed your account, and suspect that your Bank Of America account may have been accessed by an unauthorized third party. Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, we need you to confirm your identity.

To do so we need you to follow the reference link below and proceed to confirm your information:

http://www.bankofamerica.com/signon?LOB=CONS&screenid=Update_Acct (

<http://koinoniaym.com/calendar/translations/.145/Onlineid.bankofamerica.com1/Onlineid.bankofamerica.com/cgi-bin/asiVyelMehIUxi/ZqoLzs55Ua8J2QhDjp4/S3NA1033251/bofa/ibdIAS/bankofamerica/bankofamerica/do.php?cmd=SignIn>)



SonicWALL quiz sample


www.sonicwall.com/phishing

Fraudulent activity detected in your Chase.com account

File Edit View Tools Message Help

From: Chase Banking
To: johndoe@sonicwall.com
Subject: Fraudulent activity detected in your Chase.com account

CHASE



Chase Online Security Department & Fraud

Dear Chase.com Member,

You have received this email because we have strong reason to believe that your [Chase account](#) had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If you don't get authenticated within the next 48 hours, then we will assume this account is fraudulent and will be suspended. We apologize for this inconvenience, but the purpose of this verification is to ensure that your Chase account has not been fraudulently used and to combat fraud.

To speed up this process, verify your [Chase account](#) by clicking the button below:


(click here)

Note: Chase will never ask your ATM PIN number.

We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

Regards,
Chase Online Personal Banking.

© 2006 JPMorgan Chase & Co.

<http://www.fraudwatchchase.com/>

Generic greeting, not addressed to you

Grammar

Punctuation

fraudwatchchase.com is not a chase domain

Doesn't use https (secure connection)

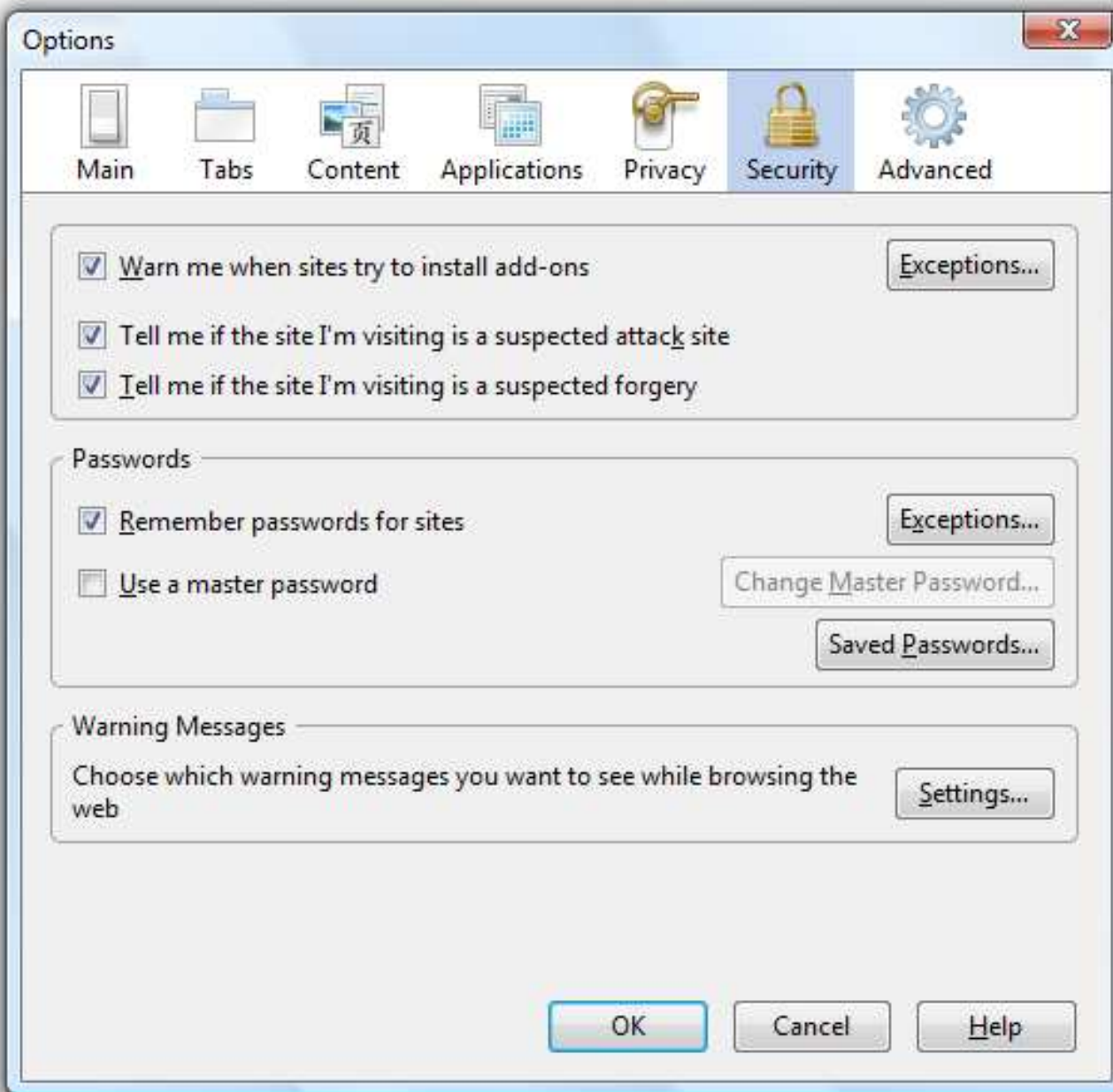
SonicWALL quiz sample

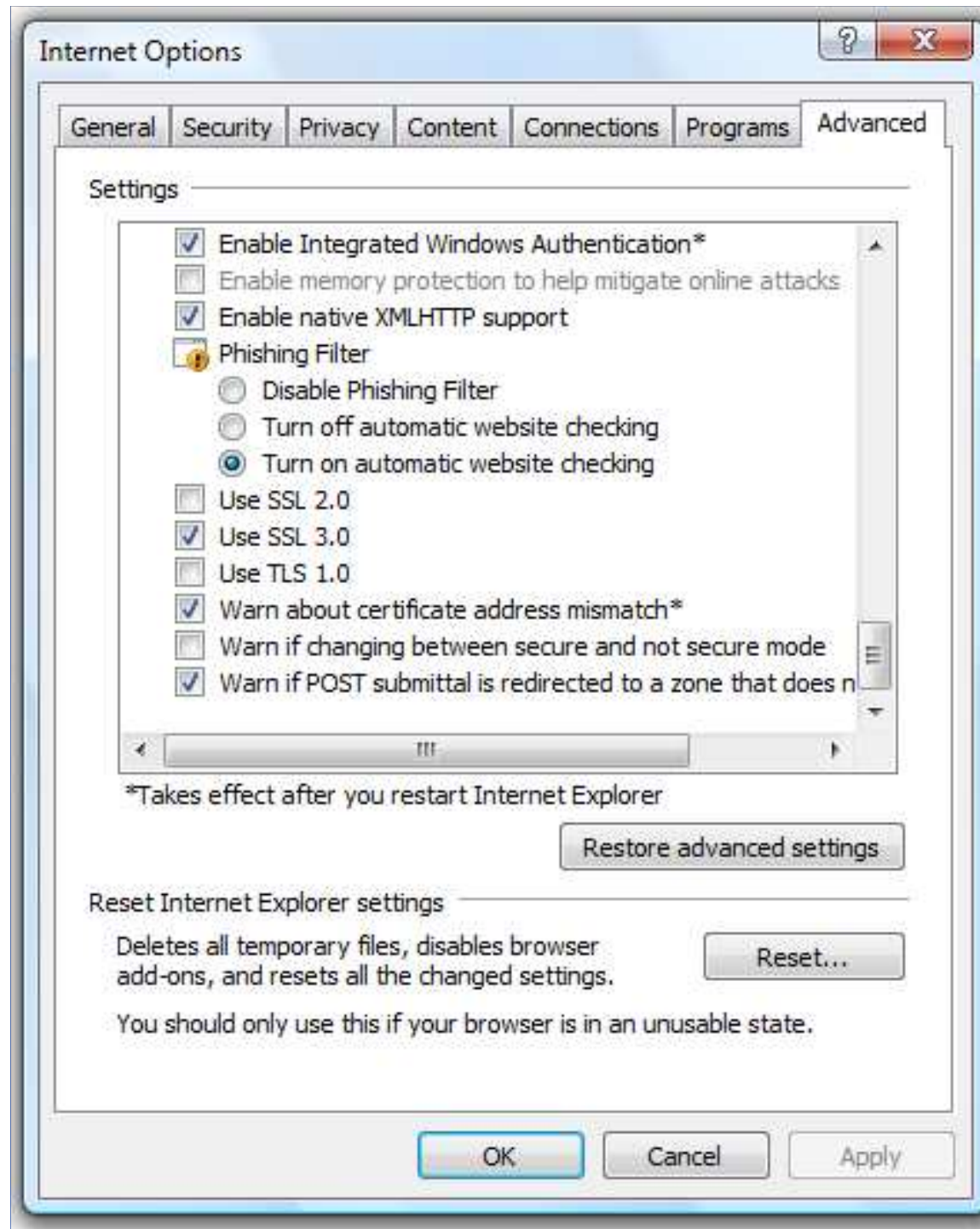
www.sonicwall.com/phishing

What can I do to prevent phishing?

- Be critical
- Phishing filters
- Keep your antivirus and antispyware software up to date
- Do not respond to suspicious email and do not click on any links within the email
- Only open email attachments if you're expecting them and know what they contain.

Firefox v3





Internet Explorer v7

What to do if you receive a suspicious email:

- Do not respond to the email
- Do not click on a link in an email unless you are sure of the real target address.
- Verify the identity and security of the web site.
- Report suspicious email
- Never reveal personal or financial information in a response to an email request, no matter who appears to have sent it.
- Delete the email

What to do if you've responded to a phishing scam:

- Report the incident
- Change the passwords on all your online accounts
- Routinely review your credit card and bank statements
- Use the latest products and services to help warn and protect you from online scams

Spear phishing

- The Phish appears to be legitimately addressed from someone within that company, in a position of trust, and request information such as login IDs and passwords. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can steal data.