

[Skip Nav](#)

U.S. Department of Education

Information for Financial Aid Professionals (IFAP) Library

[HOME](#)[Help Center](#)[What's New](#)[Schools Portal](#)[Other Links](#)[Feedback](#)[Privacy](#)

The IFAP online library contains technical publications, regulations, and policy guidance on the administration of the Federal Student Aid programs.

Publication Date: June 2006

Author: Katie Blot, Chief Information Officer

Summary: Security Alert -- Protect Against Identity Theft and Other Scams

Posted on 06-20-2006

We would like to take this opportunity to ensure that all of our Federal Student Aid partners are aware of the worldwide growing identity theft scams such as Phishing and Pharming.

Department of Education and Federal Student Aid users are not immune to these scams, and we urge you to **review carefully** the information and advice contained in this announcement and to share it with your staff as appropriate.

What is Phishing?

Phishing is a fraudulent, spoofed e-mail that looks like someone you do business with sent it. It will usually include official logos and look very authentic. The body of a Phishing e-mail may contain a message requesting that you update, validate, or verify your personal/Privacy Act protected information. The purpose of the e-mail is to get you to disclose personal/Privacy Act protected information such as PINs, social security numbers, account numbers, mother's maiden name, passwords, etc. Some e-mail may also contain links that take you to an "official looking" web site that set up a scenario in which personal/Privacy Act protected information is requested. ***These web sites may not be legitimate!***

Protecting Against Phishing E-mails

To minimize risk to yourself, if you receive Phishing e-mail:

- Never give out personally identifiable information in an e-mail or to a web site that has a link in an e-mail without validating it with the legitimate source.
- Do not open email with attachments or enclosures if they are from unknown sources.
- Do not reply to the e-mail.
- Do not type or paste any information into the e-mail.
- Do not click on any links contained within the e-mail from any unknown source.
- Use an open source tool. There are many commercial as well as free open source tools that can protect one from Phishing. A web search for "spoof guard," "Phishing protection," and "password hashing security" will reveal many of these tools. SpoofGuard and Netcraft Toolbar are only examples of the numerous products available to the public.

What is Pharming?

Pharming is the next generation of e-mail phishing attacks. However, it is not spoofing an email, it is a URL that redirects you to a fraudulent URL without your knowledge. There are several methods the pharmer uses to accomplish this, all of which are very hard to detect. You might type a valid URL in your browser only to end up at a fraudulent site that looks just like the one you thought you were going to access.

Protecting Against Pharming

To minimize risk to yourself, if you receive a Pharming URL:

- Use anti-virus software and a firewall. AVG and Zonealarm are only examples of the numerous products available to the public.
- Ensure that your browser is kept up to date and security patches are applied.
- Install a spyware detection and removal program. Ad-aware is only an example of the numerous products available to the public.
- Consider installing a Web browser tool bar to help protect you from known fraud websites. IE 7 and Netcraft Toolbar are only examples of the numerous products available to the public.
- Look for website privacy policies. Avoid doing business with any site that does not post its privacy policy.
- Limit the number of websites and amount of personal information you share on the Internet.
- Look for misspelled words and bad formatting. This may be an indication of a pharming site.
- If a password is needed, enter an incorrect password first.
- Use a reputable Internet Service Provider.

Reporting Phishing E-mails and Pharming

If you have already received or replied to a suspected Phishing e-mail that appears to be from the Department of Education, Federal Student Aid, or one of the Federal Student Aid systems or web sites (for example, the Common Origination and Disbursement (COD) web site) soliciting personal/Privacy Act protected information, please contact the Help Desk for that site so staff can investigate the e-mail. If you receive a suspected Phishing e-mail in the future, please also notify the Help Desk for that site.

If you have already received or replied to a Phishing URL or Pharming e-mail that does not appear to come from the Department of Education soliciting personal/Privacy Act protected information, you should contact the legitimate institution by telephone immediately and inform the institution of the e-mail. Attachment A provides additional information related to Phishing scams as well as additional guidance in protecting against them.

Resources

To assist you in protecting against Phishing and Pharming scams, we are attaching a document to this announcement for use by you and your staff. Attachment B is a brief summary of information about Phishing in a format that you can use to make copies suitable for posting.

Additionally, we want to make you aware of a Microsoft resource that is available to protect against Phishing scams. To check out the legitimacy of a web site-

- Replace the current URL in the address bar with the following javascript (exactly as written below).
javascript:alert("The actual URL is:\t\t" + location.protocol + "://" + location.hostname + "/" + "\n\nThe address URL is:\t\t" + location.href + "\n" + "\n\nIf the server names do not match, this may be a spoof.")
- Depress the <RETURN> or <ENTER> key.
- Compare the actual URL with the URL in the Address bar.
- If the URLs do not match, the web site is likely misrepresenting itself. In this case, you may want to close Internet Explorer.

Disclaimer

This announcement may contain information about commercial entities. Inclusion does not constitute an endorsement by the U.S. Department of Education of any products or services offered or expressed.

Contact Information

We appreciate your immediate attention to this very important issue. If you have any questions about this announcement, contact Robert Ingwalson, Federal Student Aid Chief Security Officer. He can be reached by e-mail at Robert.Ingwalson@ed.gov.

Attachments/Enclosures:

[Attachment A - "Phishing" Scam in Microsoft Word Format, Size 71KB, 8 pages](#)

[Attachment B - Prescriptions for Security in Microsoft Word Format, Size 23KB, 1 page](#)

[Home](#) | [Privacy Statement](#) | [FAQs](#) | [IFAP Search Help](#)

DRAFT

“Phishing” Scam

This information is provided to alert and educate you about Phishing scams, and provide some guidance as to steps to take to mitigate the potential damage from ID theft.

This information may contain information about commercial entities. Inclusion does not constitute an endorsement by the U.S. Department of Education of any products or services offered or expressed.

Table of Contents

[What is Phishing?](#)

[How to Avoid Phishing Scams](#)

[What To Do If You've Given Out Your Personal Financial/Privacy Act Protected Information](#)

[If you have given out your credit or debit card or ATM card information](#)

[If you have given out your bank account information](#)

[If you have downloaded a virus or Trojan](#)

[If you have given out your personal identification information](#)

[For More Information](#)

What is Phishing?

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial and/or Privacy Act protected data such as PINs, credit card numbers, account usernames and passwords, social security numbers, mother's maiden name, etc. By hijacking the trusted brands of well-known websites such as: banks, online retailers, credit card companies, and even Department of Education web sites, it is estimated that “Phishers” have been able to convince up to 5% of recipients to respond to them. Even at 5%, when you multiply by the number of recipients who receive these e-mails, that

Page 1 of 8 Page(s)

Security requires constant vigilance and is the responsibility of all employees.

becomes an awesome problem and a very expensive lesson for its victims. Our objective is to inform and hopefully prevent the exacerbation of the “Phishing” scam.

[Back to Table of Contents](#)

How to Avoid Phishing Scams

1. The number and sophistication of Phishing scams sent out to consumers is continuing to increase dramatically. While e-business is safe, as a general rule, you should be careful about giving out your personal financial/Privacy Act protected information over the Internet. The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

A. Be suspicious of any e-mail with urgent requests for personal financial/Privacy Act protected information.

(1) Unless the e-mail is digitally signed, you can't be sure it wasn't forged or 'spoofed'.

(2) Phishers typically include upsetting or exciting (but false) statements in their e-mails to get people to react immediately.

(3) They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, PINs, etc.

(4) Phisher e-mails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are.

B. Don't use the links in an e-mail to get to any web page, if you suspect the message might not be authentic.

(1) Instead, call the company/department on the telephone, or

(2) Log onto the website directly by keying in the Web address into your browser.

C. Avoid filling out forms in e-mail messages that ask for personal financial/Privacy Act protected information.

(1) You should only communicate information such as PINs, credit card numbers or account information via a secure website or the telephone.

(2) **Copy the following verbatim into the address block and <RETURN>**

```
javascript:alert("The actual URL is:\t\t" + location.protocol + "/" + location.hostname + "/" + "\n\nThe address URL is:\t\t" + location.href + "\n" + "\n\nIf the server names do not match, this may be a spoof.")
```

(3) The response will indicate whether the server name matches the URL you keyed in.

D. Always ensure that you're using a secure website when submitting credit card or other sensitive/Privacy Act protected information via your Web browser.

(1) To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just <http://>."

(2) Ensure the "lock" is visible in the lower right hand corner of your screen.

E. Consider installing a Web browser tool bar to help protect you from known phishing fraud websites.

(1) Some of the Internet Service Providers (ISPs) may offer protection against known phishing web sites.

(2) Search the internet for software products that alert you to the potential of fraudulent web sites. Some of these products may be free.

F. Regularly log into your online accounts.

(1) Don't leave it for as long as a month before you check each account.

G. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

(1) If anything is suspicious, contact your bank and all card issuers.

H. Ensure that your browser is up to date and security patches applied.

(1) MS IE users can go to the Microsoft Security home page -- <http://www.microsoft.com/security/> -- to download a special patch relating to certain phishing schemes.

I. Always report "phishing" or "spoofed" e-mails to the following groups:

(1) Forward the e-mail to the Federal Trade Commission at spam@uce.gov.

(2) Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed.

(3) When forwarding spoofed messages, always include the entire original e-mail with its original header information intact.

(4) Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/.

2. For more information, check some of the following sources:

A. For more information about how to protect yourself, see Fact Sheet 17a Identity Theft: What to do if It Happens to You at <http://www.privacyrights.org/fs/fs17a.htm>.

B. Read the information and tips put out by the Federal Trade Commission about phishing at <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>.

C. Read the Department of Justice's recent whitepaper "Special Report on Phishing" at http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf.

[Back to Table of Contents](#)

What To Do If You've Given Out Your Personal Financial/Privacy Act Protected Information

Phishing attacks are growing quite sophisticated and difficult to detect, even for the most technically savvy people. And many people are getting onto the Internet and using e-mail or Web browsers for the first time. As a result, some people are going to continue to be fooled into giving up their personal financial information in response to a phishing e-mail or on a phishing website. If you have been tricked this way, you should assume that you will become a victim of credit card fraud, bank fraud, or identity theft. Below is some advice on what to do if you are in this situation (note - some of this information is specific to United States federal laws)

[Back to Table of Contents](#)

If you have given out your credit or debit card or ATM card information

1. Report the theft of this information to the card issuer as quickly as possible (many companies/departments have toll-free numbers and 24-hour service to deal with such emergencies.)
2. Cancel your account and open a new one
3. Review your billing statements carefully after the loss (If they show any unauthorized charges, it's best to send a letter to the card issuer describing each questionable charge.)
4. Credit Card Loss or Fraudulent Charges (FCBA).
 - A. Your maximum liability under federal law for unauthorized use of your credit card is \$50.
 - B. If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use
5. ATM or Debit Card Loss or Fraudulent Transfers (EFTA).
 - A. Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
 - B. You risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you.

[Back to Table of Contents](#)

If you have given out your bank account information

- Report the theft of this information to the bank as quickly as possible
 - Cancel your account and open a new one

[Back to Table of Contents](#)

If you have downloaded a Virus or Trojan

1. Some phishing attacks use viruses and/or Trojans to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames and passwords, Social Security Numbers, etc. In this case, you should:
 - A. Install and/or update anti-virus and personal firewall software. AVG and Zonealarm are only examples of the numerous products available to the public.
 - B. Update all virus definitions and run a full scan.
 - C. Confirm every connection your firewall allows.
2. If your system appears to have been compromised, fix it and then change your password again, since you may well have transmitted the new one to the hacker.
3. Check your other accounts! The hackers may have helped themselves to many different accounts (your e-mail ISP, online bank accounts, online trading accounts, e-commerce accounts, etc.)

[Back to Table of Contents](#)

If you have given out your personal identification information

1. Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. If you have innocently given out this kind of information to a phisher, you should do the following:
 - A. Report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and do the following:
 - (1) Request that they place a fraud alert and a victim's statement in your file.
 - (2) Request a FREE copy of your credit report to check whether any accounts were opened without your consent.

(3) Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft.

B. Major Credit Bureaus.

(1) Equifax - www.equifax.com.

a. To order your report, call: 800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241.

b. To report fraud, call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241.

c. Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.

(2) Experian - www.experian.com.

a. To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen TX 75013.

b. To report fraud, call: 888-EXPERIAN (397-3742) and write: P.O. Box 9530, Allen TX 75013 TDD: 1-800-972-0322.

(3) Trans Union - www.transunion.com.

a. To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022.

b. To report fraud, call: 800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803.

2. Notify your bank(s) and ask them to flag your account and contact you regarding any unusual activity.

A. If bank accounts were set up without your consent, close them.

B. If your ATM card was stolen, get a new card, account number and PIN.

C. Contact your local police department to file a criminal report.

D. Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information.

E. Notify the Department of Motor Vehicles of your identity theft.

F. Check to see whether an unauthorized license number has been issued in your name.

G. Notify the passport office to be watch out for anyone ordering a passport in your name.

H. File a complaint with the Federal Trade Commission.

I. Ask for a free copy of "ID Theft: When Bad Things Happen in Your Good Name", a guide that will help you guard against and recover from your theft.

J. File a complaint with the Internet Fraud Complaint Center (IFCC).

(1) <http://www.ifccfbi.gov/index.asp>.

(2) The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet.

(3) For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation.

(4) Document the names and phone numbers of everyone you speak with regarding the incident. Follow-up your phone calls with letters. Keep copies of all correspondence.

[Back to Table of Contents](#)

For More Information

1. Identity Theft Help Sites:

- <http://www.consumer.gov/idtheft/>
- <http://www.identity-theft-help.us/>
- <http://www.identitytheft.org/>
- <http://www.usdoj.gov/criminal/fraud/idtheft.html>
- <http://www.ifccfbi.gov/index.asp>
- <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

2. For more information about how to protect yourself, see our Fact Sheet 17a Identity Theft: What to do if It Happens to You at www.privacyrights.org/fs/fs17a.htm.

3. Read the information and tips put out by the Federal Trade Commission about phishing at www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm.

4. Read the Department of Justice's recent whitepaper "Special Report on Phishing" at http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf

[Back to Table of Contents](#)

Prescriptions for Security

(insert local POC, phone number and e-mail address)

“Phishing” Scam

1. We have detected an increased number of “Phishing” scams sent; all Internet users are subject to “Phishing” attacks.
2. This scam comes in the form of an e-mail that “appears” to be sent by a well-known financial institution or corporation, and will usually include official logos and look authentic.
3. The body of the “Phishing” e-mail may request that you “update,” “validate,” or “verify” some personal information immediately, or your account may be deactivated or terminated.
4. The purpose of the “Phishing” e-mail is to get you to disclose personal information such as social security numbers, account numbers, passwords, UserIDs, mother’s maiden name, etc.
5. Some e-mails may also contain links that take you to an “official-looking” but illegitimate site.
6. How to protect yourself:
 - A. **Do not** reply to the e-mail.
 - B. **Do not** type or paste any information into the e-mail.
 - C. **Do not** click on any links contained within the e-mail.
 - D. **Do contact** the legitimate institution and/or the appropriate help desk/system security officer immediately. They may request that you send the suspect email to them.
 - E. **Delete** the email after following directions in 6D above.
7. If you have already replied to any of these e-mails with personal or private information, you should contact the legitimate institution by telephone immediately.

“Security is Everyone’s Responsibility”