



Session 16

Fraud Alert:

Avoiding Scholarship Scams, Phishing, and Identity Theft

Cindy Forbes Cameron

Steven Horn

Natalie Forbort (San Diego)

Steven Borders



START HERE
GO FURTHER
FEDERAL STUDENT AID



We will answer:

- What are financial aid fraud, phishing, and identity theft?
- What has ED done to help prevent further instances?
- What can FAAs do to help their students avoid these crimes?





Scholarship Scams

Cindy Forbes Cameron

Federal Student Aid Awareness &
Outreach





What types of questionable practices are out there?

- Older schemes:
 - paid search services
 - scholarships for profit
- Claims made:
 - “You can’t get this info anywhere else”
 - “We’ll do all the work”





What types of questionable practices are out there?

- More recent: financial aid “seminars”
 - general, common-sense info to group, then one-on-one sales pitch
 - claims include “the process is too complicated; you need our help”





What types of questionable practices are out there?

- More recent: payment for FAFSA submission or help
 - not always fraudulent
 - common claims are that student will miss out on maximum aid without help or that the FAFSA is too long and hard to tackle on your own





What types of questionable practices are out there?

- Most recent: the ED impostor
 - offer of a grant of up to \$8,000
 - processing fee of \$249
 - can lead to identity theft





What has ED done about financial aid fraud?

- Warnings in publications and on Web sites:
 - *Student Guide*
 - *Looking for Student Aid*
 - www.studentaid.ed.gov/LSA





What has ED done about financial aid fraud?

- Warnings at outreach events:
 - counselor conferences
 - college fairs





What has ED done about financial aid fraud?

- Report to Congress
 - released annually on May 1
 - available at www.studentaid.ed.gov/LSA
 - (click on “Note to counselors and administrators”)





What has ED done about financial aid fraud?

- Response to ED impostor scam
 - IFAP announcement, picked up by NASFAA, NACAC, many schools
 - announcements on student and counselor Web sites and in *Counselors Handbook*
 - script for CSRs at 1-800-4-FED-AID
 - warnings on listservs (FAA and counselor)
 - warnings at outreach events
 - ongoing investigation by OIG





What can FAAs do?

- Recognize the warning signs
- Distribute “Don’t get scammed on your way to college”
- Display “Don’t get stung!” poster
- Encourage students to talk to you before paying for any help or applications
- Encourage local high schools to do all of the above





Phishing

Steve Horn

Federal Student Aid Office of the
Chief Information Officer





What is phishing?

Use of **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials.

- Typical social engineering schemes use “spoofed” e-mails to direct users to counterfeit Web sites.
- Use of spyware, key loggers to capture personal data.





Dear U.S. Bank Customer,

Truth

At U.S. Bank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

Good news

At U.S. Bank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms and Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

Request

In order to further protect your account, we have introduced some new important security standards and browser requirements. U.S. Bank security systems require that your computer system is compatible with our new standards.

Threat

This security update will be effective immediately. Please [sign on](#) to U.S. Bank Online Banking in order to verify security update installation. Failure to do so may result in your account being compromised.

Anti-spam filter text

rhubarb Nelson cord

Sincerely, 8 D pawnshop dismal likewise 72 192

The U.S. Bank Security Department Team.





What Can be Done?

- Be suspicious of any e-mail with urgent requests for personal financial information
 - Unless e-mail is digitally signed, you can't be sure it wasn't forged or “spoofed”
 - Phishers typically include upsetting or exciting (but false) statements in e-mails to get people to react immediately





What Can be Done? (continued)

- They typically ask for info such as usernames, passwords, credit card numbers, Social Security numbers, etc.
- phisher e-mails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are





Phishing Prevention

- Don't use links in an e-mail to get to any Web page if you suspect the message might not be authentic
 - instead, call the company on the telephone or log onto its Web site directly by typing in the Web address in your browser





Phishing Prevention (continued)

- Avoid filling out forms in e-mail messages that ask for personal financial information
 - you should only communicate information such as credit card numbers or account information via a secure Web site or the telephone





Phishing Prevention

- Always ensure you're using a secure Web site when submitting credit card or other sensitive information via your Web browser
 - to make sure you're on a secure Web server, check the beginning of the Web address in your browser's address bar - it should be "https://" rather than just "http://"





Phishing Prevention (continued)

- Consider installing a Web browser tool bar to help protect you from known phishing fraud Web sites





Phishing Prevention

- Regularly log into your online accounts
 - don't leave it for as long as a month before you check each account
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
 - if anything is suspicious, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied





Reporting Phishing

- Always report phishing or “spoofed” e-mails to the following groups:
 - Forward the e-mail to reportphishing@antiphishing.com
 - Forward the e-mail to the Federal Trade Commission at spam@uce.gov





Reporting Phishing (continued)

- Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed (e.g. FSA help desk)
- When forwarding spoofed messages, always include the entire original e-mail with its original header information intact
- Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their Web site: www.ifccfbi.gov





Other Actions

- Spam filters
- Personal firewalls
- Trust tool bars
- Spoof protection software





Other Actions (continued)

- Always initiate the transaction
 - even if a phishing message is delivered, verify by logging to the home page directly rather than clicking the URL in the e-mail
- When in doubt always first give a wrong password
 - the legitimate URL will reject it; the phished one will accept it





What has ED done about phishing?

The Department of Education is in the process of developing communications to address phishing and pharming.





Identity theft

Natalie Forbort (San Diego)

Steven Borders

U.S. Department of Education
Office of Inspector General





ED/OIG: Who we are; what we do

- IG Act, 5 USC, appendix 3
- Organizational structure
 - Audits
 - Investigations
 - Other activities
- Reporting requirements
 - Department
 - Congress – every 6 months
 - DOJ and state law enforcement agencies





Matters of interest to OIG

Lying, cheating, and stealing

INV: ED programs

- ID theft/beneficiary fraud
- Institutional fraud
- Financial aid consultant fraud
- Employee corruption

An **intentional** distortion of the truth in an attempt to obtain something of value. Does not have to result in monetary loss.





Identity Theft – What is it?

When someone, without lawful authority, knowingly transfers or uses a “means of identification” of another person with the intent to commit, or aid or abet, any unlawful activity that violates federal law, or that constitutes a felony under any state or local law.

- Identity Theft and Assumption Deterrence Act of 1998
- 18 USC § 1028a (7)





A review of the problem

- What is the problem?
 - Fastest growing crime in the country
 - 25 million victims, 10 million in 2004
 - Sheer numbers swamp law enforcement





Further thoughts on the problem

- What's the harm?
 - 600 hours spent to restore identity and credit
 - \$1,400 out-of-pocket costs to victim
 - \$16,000 in lost productivity of victim
 - \$40,000-\$92,000 business community losses per stolen identity

Source: Identity Theft Resource Center





How do they get the information?

- Dumpster divers
- Mail thieves
- Burglary and personal theft
- Insider compromises
- Phishing
- Internet sources and hacking





How can I protect myself?

- Place passwords on credit card, bank, & phone accounts
- Don't use your mother's maiden name, birth date, last 4 digits of SSN, or phone number
- Secure personal info in your home
- Shred all documents containing your personal info





How can I protect myself? (continued)

- Drop outgoing mail in a USPS box, not your home mailbox
- Limit the number of credit cards you carry
- Don't carry your Social Security card





Web site links

- Web site provides links to federal and state resources for additional info on ID theft
 - www.idtheftcenter.org
 - www.consumer.gov/idtheft
- To opt out of prescreened credit card offers by phone, call toll-free 1-888-5-OPT-OUT
 - www.privacyrights.org





Additional Web site links

- Information on state laws, forms, and prevention checklists for businesses
 - www.idtheftcenter.org
- For identity theft brochure re: banking industry
 - www.bos.frb.org/consumer/identity/idtheft.htm





U.S. Department of Education Office of Inspector General





School responsibility

- Report fraud, waste, or abuse to the U.S. Department of Education, Office of Inspector General





School responsibility (Continued)

- 34 CFR 668.16
 1. “Examples of this type of information are –
 2.
 - (i) false claims of independent student status;
 - (ii) false claims of citizenship;
 - (iii) use of false identities;
 - (iv) forgery of signatures or certifications; and
 - (v) false statements of income; and





School responsibility (Continued)

3. Any credible information indicating that any employee, third-party servicer, or other agent of the institution that acts in a capacity that involves the administration of the Title IV, HEA programs, or the receipt of funds under those programs, may have engaged in fraud...”





20 U.S.C. § 1097 [Title IV, HEA]

- Any person who knowingly and willfully embezzles, misapplies, steals, obtains by fraud, false statement or forgery, or fails to refund any funds, assets, or property provided or insured under [Title IV, HEA] or attempts to so embezzle, misapply, steal, obtain by fraud, false statement or forgery, or fail to refund any funds, assets, or property, shall be fined...or imprisoned...





Tools used to commit identity theft of federal student aid funds

- computer
- online application process for FSA funds
- online enrollment
- identity of another person
- fake identification documents





Tools used to commit identity theft of federal student aid funds

- Selection of community colleges due to low tuition cost
- Bank accounts set up in name of identity to receive FSA funds
- Understanding of vulnerabilities of FSA programs





Identity theft FSA scheme – recent cases

- How matter was referred to our office
- Importance of working with financial aid officials
 - Receiving referrals
- Case information
 - How scheme occurred and results





Lessons learned

- FSA programs are easily vulnerable to ID theft due to lack of in-person attendance or receipt of FSA
- Subjects have extensive criminal records for theft or violent crimes
- Community colleges susceptible due to low tuition and multiple locations
- Victims of FSA fraud do not find out immediately





Lessons learned

- Easier to identify extent of fraud scheme through search warrants – subjects keep records of identities
- Need cooperation of FAAs and other agencies
- Ease of obtaining \$ for multiple subjects at same address
- Individuals are often involved in credit card and other program fraud





Protecting others from identity theft

- Properly handle documents
- Shred sensitive info
- Use key identifiers instead of the SSN
- Password-protect sensitive info
- Audit access
- Review access privileges
- View info on computers in the same manner as paper documents – is it secure?





Reducing risk

- We never know who is looking in our trash
- Shred sensitive documents
- Secure shred barrels and make sure that proper handling procedures are in place





OIG Misused Web site



“Protect your Social Security number and other personal information. Don’t let identity thieves rob you of your educational future!” – Inspector General John P. Higgins, Jr.





Thank you

We appreciate your feedback and comments.

Cindy Forbes Cameron

- e-mail: cindy.cameron@ed.gov

Srinivas Kankanahalli

- Phone: (202) 377-3361
- e-mail: srinivas.kankanahalli@ed.gov

Natalie Forbort

- Phone: (562) 980-4132
- e-mail: natalie.forbort@ed.gov

Steven Borders

