

How can I detect if my personal information is being misused?

Watch for signs that your information is being misused. These include:

- Emails, phone calls, or letters from someone claiming to be a representative of Ohio University asking you for personal information or trying to sell you “identity theft protection” products or services.
- Emails, phone calls, or letters from people or organizations you don’t know asking you for personal information.
- Emails, phone calls, or letters from people or organizations you don’t know trying to sell you “identity theft protection” products or services.

Be especially vigilant for instances of an Internet scam called “phishing.” Unscrupulous individuals create forgeries of legitimate emails and Web sites and attempt to steal your personal information using them.

The Anti-Phishing Working Group has compiled a list of recommendations you can follow to avoid becoming a victim of phishing. These include:

- Be suspicious of any email with urgent requests for personal information. Unless the email is digitally signed, you can't be sure it wasn't forged.
- Don't use the links in an email 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 the Web site directly by typing in the Web address in your browser (links in emails can be faked).
- Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as Social Security numbers, credit card numbers, or account information via a secure website or the telephone.
- Always ensure that you're using a secure network connection and 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://"

To learn more about phishing and how to protect yourself from it, read "How Not to Get Hooked by a ' Phishing' Scam".

<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

Finally, be on the lookout for warning signs of identity theft for the purpose of credit fraud. These include:

- You no longer receive your credit card statements, or you notice that not all of your mail is delivered to you. (This could mean an identity thief has taken over your account and changed your billing address to cover his/her tracks.)
- Your credit card statement includes unusual purchases.
- One of your creditors informs you that they have received an application for credit with your name and Social Security number.
- Incoming calls or letters state that you have been approved or denied by a creditor to which you never applied.
- You receive credit card, utility, or telephone statements in your name and address for which you never applied.
- A collection agency tells you they are collecting for a defaulted account established with your identity, but you never opened the account.