

## The Ohio State University Police Division

### Computer/Internet Safety Media Release

Most times when The Ohio State University Police Division is mentioned, people envision uniformed officers patrolling campus, directing traffic, taking reports, or making an arrest. The students at The Ohio State University may even be accustomed to the various programs University Police provides to promote campus safety, such as Rape Aggression Defense (RAD) classes, Student Safety Escort Services, and crime prevention in the dorms. However, most students don't think about their safety when it involves a predator that they can't see – on-line.

Did you know that there are over 60,000 computers on the Columbus campus alone<sup>1</sup>? During the day, approximately 51,500 people access the Internet using OSU networks. Depending on the day of the week and time of day, that number could easily reach 60,000-65,000 people<sup>2</sup>! As the number of users grow along with society's dependence on the Internet, it is hard to ignore the harsh reality of Internet crimes. This creates a perfect environment for criminals to prey on unsuspecting users from miles, even continents, away. The University Police want to make sure that you have the right tools and knowledge to protect yourself on-line and how to identify the warning signs of a scam so that you don't become one of the thousands of people who are victimized each day.

Here are a few tips:

- **Always be cautious when using and posting information on public sites**, such as Facebook, MySpace, EBay, Craigslist, etc. because that is exactly what they are – PUBLIC. Anyone can use the site posing as anybody to get information from you.
- **If you post an item for sale, be cautious if you get an offer for more than the asking price.** Usually, this is a warning flag for “advance fee” fraud schemes, such as the “Nigerian” or “Nigerian 419” scam. The suspect will state that some of the extra money is a “handling” or “transaction” fee and request that you send the difference back to the suspect. However, the checks they send to you are fraudulent and your bank may hold you responsible (including hefty fines) if you deposit the check.
- **NEVER give your personal information to a stranger**, unless YOU initiate contact with a verified, reputable source. This includes your name, social security number, date of birth, address, account numbers, etc. In this technologically advanced society, it doesn't take a lot of information for a savvy criminal to defraud you.
- **Be cautious of posting your personal information on the Internet.** Many people choose to post their phone numbers, “away on vacation” messages, addresses, birthdates, etc. on the Internet, where anyone, including criminals, can see. Think of it like putting your information in an ad in the newspaper.
- **Don't respond to unsolicited e-mails asking for your personal information.** Many of these “phishing” e-mails pose as banks, schools, credit card companies, etc. stating some sort of error with your account and require you to send your name, social security number, account number and other personal information to “fix” the problem.
- **Avoid using e-mail or messaging services such as IM to send personal information.** Any messages sent over the Internet can be intercepted by the wrong hands.

<sup>1</sup> The Ohio State University: Information Security Outreach / CIO IT Security Group

<sup>2</sup> The Ohio State University: Information Security Outreach / CIO IT Security Group

- **Create a strong password.** Avoid using a pet's name, birthdates, names of family members, maiden names, and obvious personal descriptors. Try incorporating upper and lower case letters, punctuation, and numbers into your password to make it difficult for others to guess. Change your password frequently and do not share them with others.

For other safe computing tips, visit:

OSU Buckeye Secure at: <http://buckeyesecure.osu.edu/>

Federal Trade Commission at: <http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm>

Federal Bureau of Investigation at: <http://www.fbi.gov/majcases/fraud/internetschemes.htm>

Internet Crime Complaint Center at: <http://www.ic3.gov/preventiontips.aspx>