National Cyber Security Awareness Month

IRM and the College of Business will present a week-long series of informational activities beginning October 18 to recognize National Cyber Security Awareness Month. The purpose of these presentations is to educate the campus community about security concerns and ways people can protect themselves online.

---

Boca Raton Campus Calendar of Events

<table>
<thead>
<tr>
<th>Monday 10/18</th>
<th>Tuesday 10/19</th>
<th>Wednesday 10/20</th>
<th>Thursday 10/21</th>
<th>Friday 10/22</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30 AM (NUR 201)</td>
<td>10:30 AM (OD 101)</td>
<td>10:30 AM (OD 101)</td>
<td>10:30 AM (OD 101)</td>
<td>10:30 AM (NUR 201)</td>
</tr>
<tr>
<td>1:30 AM (NUR 201)</td>
<td>1:30 PM (OD 101)</td>
<td>1:30 PM (NUR 201)</td>
<td>1:30 PM (OD 101)</td>
<td>12:00 PM (NUR 201)</td>
</tr>
<tr>
<td>F5: <em>Web Security—New and Rising Threats</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 PM (OD 101)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

From James Cooley,  
FAU Information Security Officer:

IRM recently formed a new division called Information Security. Our priorities in this new division include enhancing user awareness of security and better handling of sensitive information, protecting the information that the campus community entrusts to the university, and improving our infrastructure to better detect, defend, and remediate malicious threats to the university. Join us the week of October 18 on the Boca Raton campus for National Cyber Security Awareness Month activities and find out how to better protect yourself and your families.
How’s Your Game?

Gaming is one of the ways we relax and spend downtime, alone or with others. Online gaming has become a popular alternative to traditional board and card games. You can play the game you want whenever you want. You don’t need to arrange a time or place in advance or physically meet with other players.

Take these basic, common-sense measures to protect your identity when gaming online:

- Be sure your computer has an **activated and current security suite**: a firewall, anti-spyware software, and anti-virus software.
- Create a **strong password** for your gaming account. Be sure your password has at least eight characters and uses numbers, letters, and symbols.
- **Never reveal your real name**, physical location, gender, age, or other personal information to online gamers.
- Don’t post an actual picture of yourself; use an “avatar.”
- **Do not use a web-cam** when playing online.
- **Do not accept downloads** from strangers. Such programs may contain malware.

Thank You for NOT Sharing...

Facebook, MySpace, Twitter, and other social networking sites are great ways to reconnect with old school friends, share photos, and talk about the class reunion. But ill-advised postings can complicate your life in less pleasant ways. Follow these simple rules to avoid problems.

- **NEVER** reveal your year and place of birth. Those two details can be used to predict most if not all of the digits of your Social Security number.
- **NEVER** reveal your year and place of birth. Those two details can be used to predict most if not all of the digits of your Social Security number.
- **DON’T** divulge vacation plans or absences from home. What better way to invite crooks into your home than by announcing you won’t be there?
- **NEVER** reveal your home address. Of course not, you say! But recent studies show that 40% of social media site users list their home addresses on their sites.
- **DON’T** air grievances. You may have lied to get that big tax return last year or you may despise your company’s biggest client, but don’t vent about matters like these online. Revealing recreational drug use or writing about reckless behavior can cost you your job or even result in a hike in your insurance premium.
- **NEVER** reveal password clues. Typical password security questions ask for your mother’s maiden name, your city of birth, your dog’s name, or the name of your elementary school. Including information like this in your Facebook profile helps crooks guess your password.
How to Spot SPAM

In this day and age of Facebook, Twitter, and Email, scammers and malicious individuals have begun utilizing these same communication channels to trick and scam people out of their money and personal information. We need to be aware of the threats and react cautiously to messages we receive via electronic communication mechanisms.

One of the most common scams is called phishing. Phishing is a play on words to describe the act of an individual fishing for information. Phishing messages typically inform users that their account has expired, their email quota is over the limit, or that their account needs to be verified. The questions associated with the messages are often personal questions or account information.

Remember that neither FAU nor any legitimate business will ever ask you for personal information including social security number, bank account information, credit card numbers, usernames, or passwords through email or social networking services, nor will they provide a link for you to go to verify your account.

This applies to phone calls as well. If a bank asks you to verify your account information over the phone you should decline to do so, ask for the caller’s name, and call the bank using the phone number on your bank statement or the back of your credit/debit card. If the person on the other end of the phone gets upset when you decline to answer the questions initially, he is more than likely a scammer. A legitimate company representative will not get upset or angry if you take extra precautions to protect your information.

Another scam is commonly referred to as a 419 scam. These scams are called 419 scams because a lot of these scams originally started in Nigeria, and 419 was the portion of Nigerian law that criminalized these fraudulent activities. In a 419 scam, an unknown individual sends a message stating that he has come across a large sum of money (usually in the millions of dollars) and wants help to move the money. These scams work by asking you to wire money to the individual to help take care of related expenses. The scammer will even provide realistic-looking counterfeit documents upon request. These expenses usually keep increasing in cost until you run out of money or realize that it is a scam.

The safest way to deal with these messages or any of the others discussed here is to delete them.