Rice University published a series of four articles as part of National Cybersecurity Awareness Month to educate students, faculty and staff how to stay safe and be a conscientious Internet user.

Remember the 'golden rule' when handling confidential, sensitive information

The golden rule -- do unto others as you would have them do unto you -- is sound advice, even in the context of the cyberworld.

Rice faculty, staff and even some students are entrusted to handle protected, private information every day, from student and health records to bank account and credit card information to employee data. “We should protect this information just as we expect others to handle our private information correctly and safely,” said Marc Scarborough, chief information security officer for Rice's Office of Information Technology.

Employees have been trained on how to handle this kind of information and how to recognize it, and departmental policies and procedures are in place to help protect the information consistently. Rice University Policy 808 describes what kind of data is protected. Protected data is classified as confidential and sensitive. The general distinction between the two is simple: Information that has legal protection obligations, like Social Security numbers and student records, is classified as “confidential.” Proprietary and internal information, like employee IDs and university infrastructure information, is classified as “sensitive.”

"We must use caution when receiving, handling and storing private information," Scarborough said. He offered these tips for best practices:

- Train new additions to departments when they arrive (and, in some cases, annually).

- When data appears in places where it would not normally appear, like an unencrypted email or in a public Google search result, report it to the Information Security Office (itso-l@rice.edu or 713-348-5735).

- If you have questions about the best ways to receive, store and send protected information, contact the Information Security Office to learn how tools and technology can be used to safeguard confidential and sensitive information.

"We handle private information every day," Scarborough said. "Not only must we protect this information, but we also have an obligation to let someone know if we see an issue with how protected information is handled or if we make a mistake ourselves. We should be timely in our reporting. The longer a record remains in the open, the longer it remains at risk."

For more information about Rice IT Security, visit http://it.rice.edu/security/. For information about National Cybersecurity Awareness Month, visit www.staysafeonline.org.

Lock it down: Keep digital accounts secure with strong passwords

What would you do if you lost access to everything in your digital world? Consider this scenario: Your emails, contacts, documents and even photos are out of reach -- or worse, being deleted. Your passwords to all your accounts have been changed. Your contacts are receiving unwanted or even harmful emails from you -- or so they think.

If someone steals your password, it could happen.

Passwords have a single purpose: to protect a resource. Generally speaking, a password's strength -- its length and complexity -- as well as how often it is changed should be directly related to the value of the resource it's protecting.

In a single sign-on environment like Rice, where one password is used for everything -- from checking email to accessing Rice's virtual private network to using departmental shares -- passwords should be strong. They should include numbers, symbols, capital and lowercase letters, and they should be changed periodically.

For some resources, another option is "multifactor authentication," or MFA. This type of authentication can help protect accounts even if a password is stolen. Much like a bank ATM requires both a card and a PIN to access an account, MFA requires at least two forms of authentication before access is allowed. Rice Google accounts, for example, can be configured to use not only a password, but also a unique, one-time code sent to a user's mobile phone. Google calls it "Google Two-Step." If an attacker does steal a user's password, the villain will not be able to log into the Google account; the attacker will not have the one-time, unique code sent to the user's mobile phone.

Twitter and Facebook have similar technologies that can be enabled for that extra layer of logon security.

"Rice is also looking at providing MFA to some sites on campus," said Marc Scarborough, chief information security officer for Rice's Office of Information Technology. "We are currently piloting technology similar to what Google and Facebook offer -- a way to further enhance the logon security of some of our Web-based applications. We are partnering with Duo Security to provide MFA to these sites and services. As we move forward in our pilot and implementation, we will provide more information."

Until then, Scarborough recommends these best practices:

- Enable extra security options when available.
- Enable Google Two-Step authentication on your Rice Google account.
- Choose different passwords for different sites. Using the same password in multiple locations, even though convenient, lowers the security of those services. If one of them has a breach, then that stolen password will work everywhere it's used.
- If you have access to confidential and sensitive information, change your password at least once a year.

"Passwords are everywhere," Scarborough said. "For every new service we use, we have to create a new password. It also seems as if we see a new service breach every time we read the news. Password theft, through phishing, stolen account databases and keystroke-logging malware, are becoming more common. As companies offer better tools to secure our accounts, we should take advantage of them."

Spear phishing: Don't take the bait

It seemed like an ordinary request: A Rice employee got an email from a colleague asking for university bank account numbers. Fortunately, rather than simply hit reply, the employee picked up the phone -- and that's when the jig was up.

The email was a convincing spear-phishing attack targeted at stealing financial information.

"What made the email look so convincing was that it appeared to come from someone the victim knew and someone from whom the request would seem normal," said Marc Scarborough, chief information security officer for Rice's Office of Information Technology. "The attacker in this case actually took the time to learn Rice's reporting structure and crafted a targeted email message to a single person."

The "From" address on an email is easily forged. It's essentially the same as a return address on a postal envelope. People generally write an accurate return address, but anything can be written there. That's true for emails as well. And it's even harder to detect a forged "From" address on a mobile device since less information is shown on smaller screens.

"We should be aware that not all emails we receive are from whom they say they are," Scarborough said. "If an email requesting information appears unusual, even if it appears to be coming from someone you know, take the time to investigate. Call the person who supposedly sent the message. Find out if they really did request the information before you send it, whether it's banking information or any other type of private information -- account information, student

information or general information about your department’s operations.

"Not all phishing emails are the same. Some are more than the poorly worded emails asking for our passwords that we’re used to. Attackers are getting much better at learning about us to make their attacks more successful."

If you're at all suspicious about an email, it's probably a scam. No one at Rice will ever ask you to verify your NetID account or ask for your password, ID number, credit card information or other personal details by email.

If you fall for a phishing message, immediately contact the Help Desk, helpdesk@rice.edu or 713-348-HELP (4357), to reset your password.

Safeguard mobile devices

Mobile devices like laptops, smartphones and tablets help people be more productive and connected than ever before. But the very features that make these devices so handy also make them a security risk.

Rice employees report lost or stolen devices several times a year. Whether forgotten at the airport or swiped during a break-in, lost devices cause frustration and anxiety -- not only for the employee but for the university as well.

If the device contained private information and was not properly protected through encryption or other tools, the university could be at risk. Regardless of whether the data was lost or stolen, Rice has legal obligations to those affected. These obligations are not only difficult to adhere to but can be very expensive.

"People are often unaware that their device contains confidential and sensitive information," said Marc Scarborough, chief information security officer for Rice's Office of Information Technology. "Emailed documents are often cached in email programs, temporary files created while working on documents are sometimes not deleted and many times people work on documents that contain protected information without even realizing it."

Even data that isn't considered confidential or sensitive can be a tough blow if lost. Recreating that work is frustrating and time-consuming.

Scarborough recommended these actions:

- Take care of the security of mobile devices. Use the tools available to properly protect devices, including backup software like Crashplan for Rice; encryption, like BitLocker from Microsoft and File Vault from Apple; personally identifiable information (PII) detection software, like Identity Finder; and virtual private network, or VPN.

- Enable the security protections offered by mobile devices such as "remote wipe and kill" from services like iCloud.

- Be aware of surroundings when traveling with devices. Keep devices out of sight in cars, and don’t leave them unguarded in restaurants, libraries and other public places.

If one of your devices used for Rice-related activities is lost or stolen, Scarborough said, report the theft to the local police. If the device is owned by Rice University, report the theft to Rice University Police Department as well. The police will ask for the make, model and serial numbers of the stolen devices. If you don't have them available, get the case number from the responding officer so you can call back with the information to update the case file. Finally, report the loss or theft to your department and to the Rice IT Security Office, security@rice.edu.

For more information or help in ensuring your devices are secure, contact the Help Desk at helpdesk@rice.edu or 713-348-HELP (4357) or visit http://infosecurity.rice.edu/.