Outdated Technology Makes Hampton Vulnerable to Hackers: Puts students and staff at risk

Posted At : December 7, 2018 3:20 PM | Posted By : Mavis Carr
Related Categories: Technology

By Mark Edwards

Hampton University's technological infrastructure is grossly outdated and allows for multiple vulnerabilities that put students, staff, and the university at risk. The system is so easily hacked, it allows anyone with a basic understanding of computer science can get into its secure areas.

"I really can just take anything if I wanted to," said Wesley Freeman, a senior computer science major.

Armed with only basic social engineering to get users' personal information, hackers can then access their accounts. Outdated software provides a window into servers. Password and ID numbers are often visible when logging in to student resources making them readily available to hackers, according to multiple computer science majors and cyber security professor Dr. Danny Barnes. Because Hampton runs an unsecure network, eavesdroppers can observe on-screen activity from a different location.

A hacker with just a person's name can access that person's personal information. For example, a Google search for "Hampton password recovery" leads to Hampton University's password reset page. Entering a name and answering two security questions, allows the password to be reset. The new password gives access to the person's Blackboard account, university email, and provides a portal to their Touchnet, the website used to track and make payments on student accounts.

Answers to security questions are often easily found on social media like Facebook, Twitter or Instagram. Social media often includes things like birthdays, states where people were born and the names of pets. Also, in the Hampton system, if users can't answer the first set of security questions, they can keep refreshing until they find a question they can answer.

"It's crippling easy (to use social engineering). All you need is someone's Facebook," said one computer science student.

Computer experts recommend not using Hampton's auto-generated security questions, suggesting instead that password resets be controlled by administrators. For instance, the name "William Harvey" appears four times on the password reset page. None have security questions associated with them, making it unlikely anyone could reset the password electronically. Those who don't use security questions must appear in person at the library

to have their password reset.

People who understand code can get further into Hampton's system, because there is a pattern to how student ID numbers, blackboard and InfoTech passwords are created. Each fall semester, administrators announce the standardized InfoTech password to a room full of freshman. Students can change their password at any time, but it automatically resets to the old password after a period of time.

"That's bad," Dr. Barnes said. "People can go in periodically and keep trying standard passwords that they knew were set at the beginning."

Hampton's standardized password has a minimum of six characters, but programs are readily available that can determine passwords with up to 15 characters. The predictability of these passwords helps the programs work faster.

BlackBoard passwords share this vulnerability because the BlackBoard website uses the university ID number as the user name. Then, the login page tells the user that the password is the first initial of the first and last name of the user followed by the last four numbers of the ID number. At least some university computers provide a dropdown menu of previous user ID numbers, essentially providing a foolproof means for logging in.

"They need a randomizer when they generate your generic or your login password," Dr. Barnes said. "I don't know why we don't have one yet."

A password randomizer does not follow such an easily hacked pattern. Instead, it randomly assigns characters. In addition, it can generate secure passwords over 15 characters, making it more difficult for a password-identifying program to crack. A randomizer would help protect students and staff from malicious programs.

Account security is just one of many vulnerabilities of the university's system. The technological infrastructure is also problematic. The server architecture makes it difficult to update the thousands of computers across campus. Outdated computers are dangerous because they can allow access into the server. An unprotected server leaves the entire system vulnerable to collapse.

Hampton runs on a client-server architecture, Barnes said. This means every staff computer is directly linked to the main server. If someone hacks one computer, they can get into the main server.

Dr. Barnes recommends a "thin-client architecture." This would let information from the server come to computers without putting the server at risk and would save Hampton money in the long run.

"If I need a new piece of software, what they have to do now is come to this terminal and upgrade it," said Barnes, "if we were on a thin-client architecture, all I'd have to do is put it on the server and push it to all the computers."

Pushing upgrades out fast is important for security. Many computers on campus run on outdated operating systems like Windows 7. They no-longer

release patches for these software and known vulnerabilities are easily searchable.

Hampton's security issues follow a pattern of outdated systems that allow a laundry list of vulnerabilities. In some cases, Hampton can't enforce its own Appropriate Use of Technology Policy.

For instance, blocked websites can be accessed with a few tricks, like quickly refreshing the screen. In addition, programs can perform this task automatically. The university Wi-Fi can also be accessed during random grace periods when no password is required, making it available to the public, according to one computer science student.

It's difficult for students to feel safe on Hampton's network and the university doesn't allow students to have personal routers on campus. A personal router allows users to be on a more private network, making it less likely they could be hacked. Some students use their computers as personal hotspots, filtering Hampton's Wi-Fi through their computer to bypass Hampton's server restrictions. This provides a level of security that helps protects them from being hacked through the Hampton system. But, it also allows them to bypass university restrictions.

"I don't know how to protect myself on Hampton's internet," Rabekkah Maxwell a Sophomore kinesiology major.

Dr. Barnes recommends using a passphrase, a memorable sentence the user doesn't share with anyone and that has no personal affiliation.

"Going into a thin-client or a zero-client architecture and improving our Wi-Fi are the biggest things we can do on the electronic side that I that would help," Dr. Barnes said.