UNC | SCHOOL OF DENTISTRY
Computing and Information Systems

July 2018

OUCH! NEWSLETTER

Phone Call Scams/Attacks

This month's OUCH newsletter is about phone call scams and attacks. These attacks are part of hacking called social engineering.

The article below explains how phone call scams work, the easiest ways to detect them and how to respond if you do get attacked.

Read more about phone scams and attacks here.

Security Awareness Training Test Requirement

In order to comply with HIPAA and UNC policy, OCIS is enforcing the annual School of Dentistry Security Awareness Training requirement.

You will be **required** to take and pass both the HIPAA and Security Awareness test in

Laptop Encryption Project Status

It is not enough for your laptop to be encrypted, we must have documentation and proof of encryption in the event your laptop is lost or stolen.

OCIS has documented the encryption of **403** laptops, and validated the encryption of **191** laptops. If your laptop does not have a tag like the one above, OCIS may not have a record of it. Please bring your laptop to OCIS immediately for a security check.

REMEMBER: If you have an unencrypted laptop or unencrypted USB flash drive and are using it at the school, contact OCIS as soon as possible! *Failure to do so is a violation of HIPAA and University policy.* Don't get caught with an unencrypted device.

Phishing

OCIS still receives reports of phishing attempts. **To better spot phishing, click here.**

Please forward any phishing messages that you encounter **as an attachment** to

order to access the EPR.

To take the Security Awareness Training and Test **please click here.** If you have questions, please contact OCIS.

ATTENTION: Two-Step Authentication is Coming

Recent events at the University are forcing campus to accelerate 2-step authentication for all Office 365 users as early as September or October 2018.

ALL incoming 2018 students will be required to register for 2-step to access Office 365 - this means incoming DDS, DH and graduate students.

Here is the upcoming two-step schedule:

- **Fall 2018:** Required for students in Office 365
- **TBD (September or October 2018):** Required for faculty and staff in Office 365 (*currently optional*)

To set up your two-step, go to **its.unc.edu/2-step/.**

If you have any questions, contact OCIS.

How to Create a Secure Password

Your password is your defense against

phish@unc.edu.

For an explanation of how to forward an email as an attachment **please read the following article on help.unc.edu.**

To check and see if you have a suspected phishing email, go to **its.unc.edu/phish-alerts/.**

US DHHS Office of Civil Rights in Action

Guidance on Software Vulnerabilities and Patching

Many HIPAA covered entities (like the School of Dentistry) and business associates are highly dependent on software for processing and handling of electronic protected health information (ePHI).

Under the HIPAA Security Rule, both are required to protect their ePHI, which includes identifying and mitigating vulnerabilities of computer programs and systems that could affect the security of ePHI.

Identifying software vulnerabilities and mitigating the associated risks are important activities to conduct as part of the security management process and technical evaluation.

Password Managers

A password manager helps to generate and retrieve complex passwords, potentially storing such passwords in an

cyber-criminals. It is important that you choose a long and strong password that cannot be easily cracked. This is especially important for in health care environments like the School of Dentistry.

Click here for the OCIS recommended guidelines for choosing an effective password.

encrypted database or calculating them on demand.

When selecting a password manager for your personal use, **the UNC-CH Information Security Office recommends you use the matrix given here** to evaluate the relative strength of any password manager under consideration.

HIPAA Security Incident Update

The School of Dentistry has gone **1** day since the last reported HIPAA security incident. In the last 30 days, OCIS has found a compromised Office365 account and discovered **advanced persistent malware**.
Please stay vigilant!

OUCH! Archives
Click here for prior issues and topics.

Security Awareness Tip of the Day

Remember, it is your personal responsibility to protect patient data (e.g., electronic Protected Health Information) on laptop computers and portable media devices (e.g., CD/DVDs, USB keys, USB drives and SD cards). In all cases, patient data can never be stored on a portable computing or media storage device unless it has been inventoried, encrypted and approved by OCIS.

Contact Us

School of Dentistry HIPAA Security Officer
David Rankin
Email: **david_rankin@unc.edu**
Phone: (919) 537-3485

School of Dentistry HIPAA Privacy Officer (Interim)
Dr. Lisa Stoner
Email: **lisa_stoner@unc.edu**
Phone: (919) 537-3588

School of Dentistry Deputy Security Officer
Mauricio Tavares
Email: **mtavares@unc.edu**
Phone: (919) 537-3428

School of Dentistry Risk Management Officer
Martin Folliard
Email: **mfolliar@email.unc.edu**
Phone: (919) 537-3444

For More Information

School of Dentistry Policies | UNC-CH Policies | What is Sensitive Information?

The Office of Computing & Information Systems (OCIS)
(919) 537-3500
OCIS-Help@ unc.edu
http://bit.ly/UNC-OCIS

Connect with us