UNC | SCHOOL OF DENTISTRY
Computing and Information Systems

June 2018

OUCH! NEWSLETTER

Stop That Malware!

You probably have heard of terms such as virus, Trojan, ransomware, or rootkit. These are different types of malicious programs called **malware** that cyber criminals use to infect computers and devices. Once installed, they can do whatever they want.

Learn what malware is, what danger it poses, and most importantly, what you can do to protect yourself from it here.

Security Awareness Training Test Requirement

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 **phish@unc.edu**. For an explanation of how to forward an email as an attachment

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 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

Campus networking and security have notified OCIS that two-step authentication is now required (effective January 2, 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 (*currently optional*)
- **Spring 2019:** 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.

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

Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations

A U.S. Department of Health and Human Services Administrative Law Judge (ALJ) has ruled that The University of Texas MD Anderson Cancer Center violated HIPAA, requiring MD Anderson to pay $4.3 million in penalties. This is the fourth largest amount ever awarded or secured in a settlement for HIPAA violations. MD Anderson had three separate HIPAA data breaches in 2012 and 2013 involving the theft of an unencrypted laptop from the residence of an employee and the loss of two unencrypted thumb drives containing the unencrypted electronic protected health information (ePHI) of over 33,500 individuals.

New Guidance on HIPAA and Individual Authorization of Uses and Disclosures of PHI for Research

OCR has issued new guidance on HIPAA and individual authorization of uses and disclosures of protected health information (PHI) for research. This guidance explains certain requirements for an authorization to use or disclose PHI for future research. It also clarifies aspects of the individual's right to revoke an authorization for research uses and disclosures of PHI.

How to Create a Secure Password

Your password is your defense against 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.

Password Managers

A password manager helps to generate and retrieve complex passwords, potentially storing such passwords in an 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 **64** days since the last reported HIPAA security incident.
Good job and 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**

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

Phone: (919) 537-3485

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

Phone: (919) 537-3588

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