ATTENTION: Two-Step Authentication is here!

Starting in November, faculty and staff will be required to have 2-step to use Office 365. Click here for the roll out schedules for both students and faculty/staff.

Everyone is encouraged to enroll as soon as possible to avoid any issues with Office365 applications (Heelmail, Microsoft Office, etc.).

To set up your 2-step, go to its.unc.edu/2-step/. If you have any questions, contact OCIS.

Please note, staff members with a student affiliation (i.e. enrolled in a course or program) will be included in the student activation. Faculty/staff accounts will be enforced according to their earliest possible affiliation. For example, if you are a faculty member with dual appointment in two different schools, your 2-Step will be activated with the school switching over first, even if you don't consider this your primary affiliation.

HOW TO SET UP 2-STEP FOR OFFICE 365

Step 1: Visit onyen.unc.edu and click on “2-Step Verification for Office 365.”

Step 2: Follow the quick on-screen prompts to opt in to 2-Step Verification.

Step 3: Visit office.unc.edu to finish 2-Step enrollment. Note: you will need your mobile device to complete this step!

TOP TIP:

Do you use a non-Microsoft app to check your Heelmail on your phone?

If so, you will need to get an “app password” during Step 3 of the enrollment process. You’ll need to enter this code in your email app to keep receiving your messages.

If you miss this during the enrollment process, visit the “Security & Privacy” section of your account settings. Then, click on “Additional security verification.” A tab for app passwords can be found there.
Compromise (BEC)

Attacks have developed an email attack called CEO Fraud, or Business Email Compromise (BEC). These are targeted attacks that trick their victims into taking an action they should not take. What makes these attacks so dangerous is cyber attackers research their victims before launching their attack. Read more here.

Email Oops, and How to Avoid Them

Second, sometimes we can all be our own worst enemy with email. Email features such as auto-complete can be both confusing and can cause more harm than any hacker. Read this article to learn how to avoid the most common email mistakes and make the most of email. Read more here.

Security Awareness Training Test Requirement

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

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 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/.
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.

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.

US DHHS Office of Civil Rights in Action

The US DHHS OCR reached settlements with Boston Medical Center, Brigham and Women’s Hospital, and Massachusetts General Hospital for HIPAA violations by inviting film crews on site to film “Boston Med,” an ABC television network documentary series, without first obtaining authorization from patients. Collectively, the three entities paid $999,000 to settle HIPAA privacy violations. To read more about this case, click here.

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 61 days since the last reported HIPAA security incident. 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 Deputy Security Officer
Mauricio Tavares
Email: mtavares@unc.edu
Phone: (919) 537-3428

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

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

For More Information

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