Dear Carolina Community,

I am writing to inform you of our plans to expand the use of 2-Step Verification on campus in 2018. This continues the work that ITS has already completed to put select digital resources, such as the online W2, VPN and administrative IT applications, behind 2-Step Verification protection. A great many in our community are routinely using 2-Step Verification successfully today.

We do, however, need 2-Step Verification in more places. As many of you saw over the 2017 Thanksgiving break, criminals continue to use phishing messages to access accounts. This is true at UNC-Chapel Hill and across higher education. In November 2017, phishers successfully compromised several hundred Onyens and passwords by phishing student, faculty and staff accounts. Criminals used that access to launch thousands of additional attacks here on campus. 2-Step Verification would have stopped these attacks, saved our community the headaches associated with re-authenticating accounts, and saved the University time and money.

What is 2-Step Verification?

2-Step Verification -- also called multifactor or two-factor authentication -- is an additional layer of protection for your accounts. 2-Step Verification utilizes something you know (your Onyen and password) and something you have (e.g. your phone).

Many of you are likely already using 2-Step Verification for online activity with bank accounts, credit cards and personal email accounts. If you've received a code sent to your phone before you could sign in to an account, you have used 2-Step Verification.

Why is 2-Step Verification Important?

The main benefit of activating 2-Step is that it significantly increases the protection of your account from hackers. Here's how that is achieved:

- 2-Step adds an extra barrier between your personal information and unwarranted access. To access your account, criminals would need to know your username and password as well as a security code;
- 2-Step can help keep criminals from accessing your email, documents, payroll, personal information or research data, even if your Onyen and password have been stolen;
- 2-Step requires a unique security code each time your account is accessed on a non-trusted device, application or web browser.

Action Required

Our 2018 implementations begin with a focus on student use of Office 365 and ConnectCarolina access. In the coming weeks and months, students will hear more about 2-Step Verification, including how to activate 2-Step, how to set up devices, how to find support and other valuable information. Students should pay close attention to those messages, as they will provide essential instructions for securing accounts. Faculty and staff will hear more about expanded use of 2-Step later this year.

We all have a role in protecting the digital assets and resources of the University. We appreciate your support and collaboration as we introduce additional digital security measures to keep our campus safe.

Regards,

Chris Kielt

Vice Chancellor for Information Technology and Chief Information Officer

This message is sponsored by: Information Technology Services