NC STATE UNIVERSITY

5 Tips to Avoid Phishing Attacks

Phishing attacks are on the rise at NC State. Spammers are targeting your university and personal accounts in an attempt to steal your identity. Don't get compromised. Protect yourself and your accounts by following these 5 simple tips.

1. Never send sensitive info in email

- Protect your SSN, usernames, passwords, credit card and bank account information, etc.
- NC State IT staff will **NEVER** ask for your Unity password via phone or email.
- To learn more, visit: go.ncsu.edu/data-framework

2. Activate Google's 2-Step Verification

- Add another layer of security to your documents, email, and account information.
- Request security codes and approve devices.
- Visit go.ncsu.edu/2-step to learn more.

3. Install Antivirus

- NC State provides *free* antivirus software.
- Download and install antivirus on your device: go.ncsu.edu/antivirus

4. Avoid opening attachments from senders you don't know

- Delete an email if you don't recognize the sender's name or if it looks suspicious.
- Delete an email if you aren't expecting attachments.
- Play it safe and use common sense.

5. Verify hyperlinks

- Hover over a link in an email to view its destination and verify it is safe.
- Review the *entire* url to confirm legitimacy.
- DO NOT CLICK on suspicious links or links you don't recognize.

Questions about Phishing?
Contact the NC State Help Desk at 919.515-HELP (4357) or help@ncsu.edu; or
Visit go.ncsu.edu/avoid-phishing

oit