secure U

Recognize and Report Email Scams

WHAT IS PHISHING?

Phishing refers to deceptive emails that can lead to theft of personal information or University data.

It is important to make security a priority and protect your information and the information of others.

Phishing emails attempt to get you to share personal information, such as passwords, social security numbers, or bank information.

Protect yourself from phishing attempts by thinking twice before you click, keeping current on recent or common phishing scams, and immediately reporting suspicious emails or phone calls to the University for investigation.

PHISHING EMAILS CAN...

- Appear to come from anyone, including "UMN Edu Team," "Service," "HelpDesk," "Customer Service," or even a colleague, professor, or friend whose account has been compromised.
- Include threats or dire consequences if you don't act quickly.
- Ask you to open a shared document you may or may not be expecting.
- Link to a login page that may or may not look like the University's login page, but the web address does not end in ".umn.edu." It may also be shortened by services like tinyURL, or look like Google or Dropbox.

ACT QUICKLY

if you suspect you have responded to a phishing email or clicked on a link in error

REMEMBER

the University will never ask you to provide your username and password via email

CHANGE

your University internet password and account secrets.
For help, contact UMN Technology Help at 612-301-4357 or **help@umn.edu**

LEARN

more about recent and common phishing scams at **phishing.it.umn.edu**

REPORT

any suspicious activity or uncertainty regarding email messages to **phishing@umn.edu**

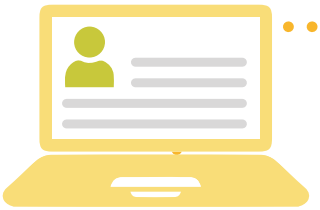
QUESTIONS?

Contact the Information Security team at **security@umn.edu** or visit **it.umn.edu/safe-computing**

Protect Yourself Against Identity Theft

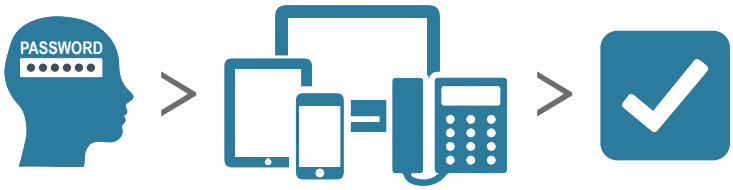
You have the power to protect yourself!

Do not duplicate passwords between personal and professional accounts, and do not share your passwords. Learn more: **z.umn.edu/passwords.**



Regularly review your online accounts such as financial statements and social media.

Use two-factor authentication tools wherever you can. **Use Duo at the University of Minnesota to protect your direct deposit and W-2 information.**



Opt in today: **z.umn.edu/duoprotection**

Recognize and report email scams to **phishing@umn.edu.**

In case of suspected theft, act quickly. Contact the University of Minnesota Help Desk at **help@umn.edu** or **612-301-4357** and visit **IdentityTheft.gov** for next steps.

Clues that someone has stolen your information

- You see withdrawals from your bank account that you can't explain or you find unfamiliar accounts or charges on your credit report.
- Debt collectors call you about debts that aren't yours.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- Medical providers bill you for services you didn't use.
- You receive a notice that your information was compromised by a data breach at a company where you do business or have an account.
- Your wallet, Social Security card or number, or other personal data has been lost or stolen.