Things to know about
PHISHING at UW

WHAT IS IT?

Phishing is a form of email fraud in which potential victims are enticed into providing sensitive information or login credentials, which can then be used to access personal and UW institutional information.

EXAMPLES

Phishing emails arrive in many forms. Common characteristics include:

Subject: Account storage exceeded

Your mailbox is almost full.

Dear User,
Because of space limitations, you will soon be unable to access your account.
Click here to automatically increase your account storage.

Kindly,
Mail System Administrator

Subject: Verify Your Account

BESTBANK

Dear Customer,
Your contact information is out of date. So that we may better serve you, please attend to this matter by clicking on the link below.

Verify Your Account

BEST BANK

fakeyurl.abc?qrzz7%9l

The resource you requested requires you to log in with your UW NetID and password.

UW NetID

Password

They create a sense of urgency

Sometimes the emails will compel you to act quickly by threatening to cut off access to accounts, systems, or other resources.

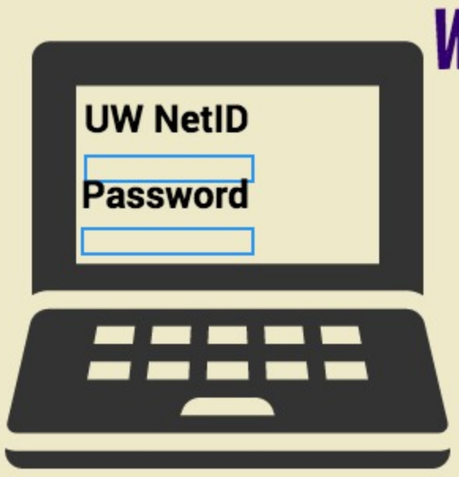
They may appear "official"

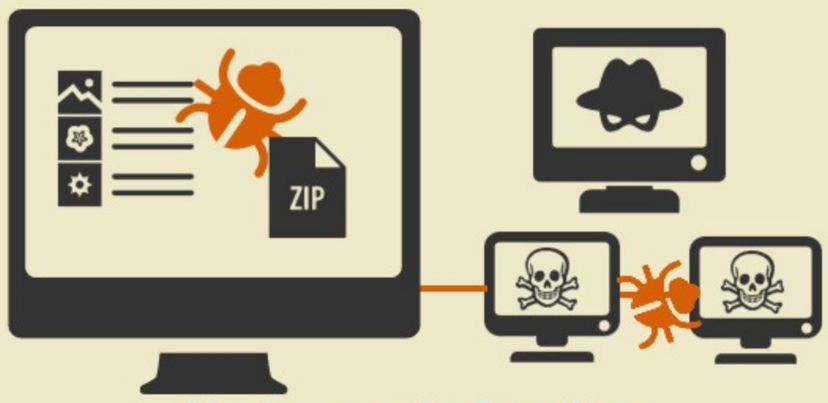
Phishers often use logos, colors, and other visuals associated with well-known brands to trick recipients into providing information.

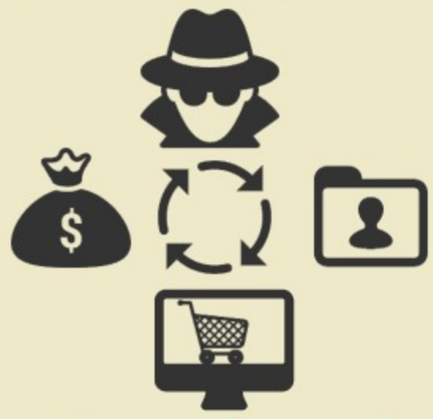
They may ask you for info

If an email urges you to click on a link that asks for your UW NetID password or other credentials, it could be a phishing attempt.

WHAT HAPPENS IF YOU CLICK ON A LINK IN A PHISHING EMAIL ?







Unauthorized access

Stolen credentials and passwords may be used to access personal data, such as financial information, and University information systems and resources.

Malware infection

Clicking on a link in email may lead to a malware infection on your computer. It may be used to collect data, add spyware to your machine, and/or connect it to a network of infected systems known as a botnet. (See the Office of the CISO's "Things to Know About Malware" infographic.)

Feeding the cyber crime cycle

Cyber criminals have a sophisticated underground market where all types of personal data may be bought and sold for cash.

YOU JUST GOT A SUSPICIOUS EMAIL– WHAT SHOULD YOU DO?

1 Do NOT click on any links

2 Forward the message as an attachment to help@uw.edu

UW Medicine employees should cc uwmed-abuse@uw.edu

HOW CAN YOU PROTECT YOURSELF?

Update and patch

Keep operating systems, software, browsers, and plug-ins updated and patched on your computers and devices.
Learn more:
ciso.uw.edu/update-and-patch

Use antivirus software

Sophos Anti-Virus Software is available free of charge to all UW students, faculty, and staff. More info:
washington.edu/itconnect/wares/uware/sophos-anti-virus-software

Employ good password practices

Passwords online training:
ciso.uw.edu/online-training/#passwords

Never click on links or download attachments unless you can verify the source

Phishing training and guidance:
ciso.uw.edu/resources/risk-advisories/phishing

Use encryption on files, devices, and communications whenever appropriate.

Encryption guidance:
ciso.uw.edu/resources/privacy-briefs/encryption

Back up your data

Back up all data that you are responsible for in case of loss or corruption due to phishing or malware infection.

RESOURCES

Phishing Risk Advisory - ciso.uw.edu/resources/risk-advisories/phishing/
IT Connect - Secure Your Computer https://itconnect.uw.edu/security/securing-computer/

Office of the Chief Information Security Officer
University of Washington

More info: ciso.uw.edu/online-training/#phishing
Home page: ciso.uw.edu