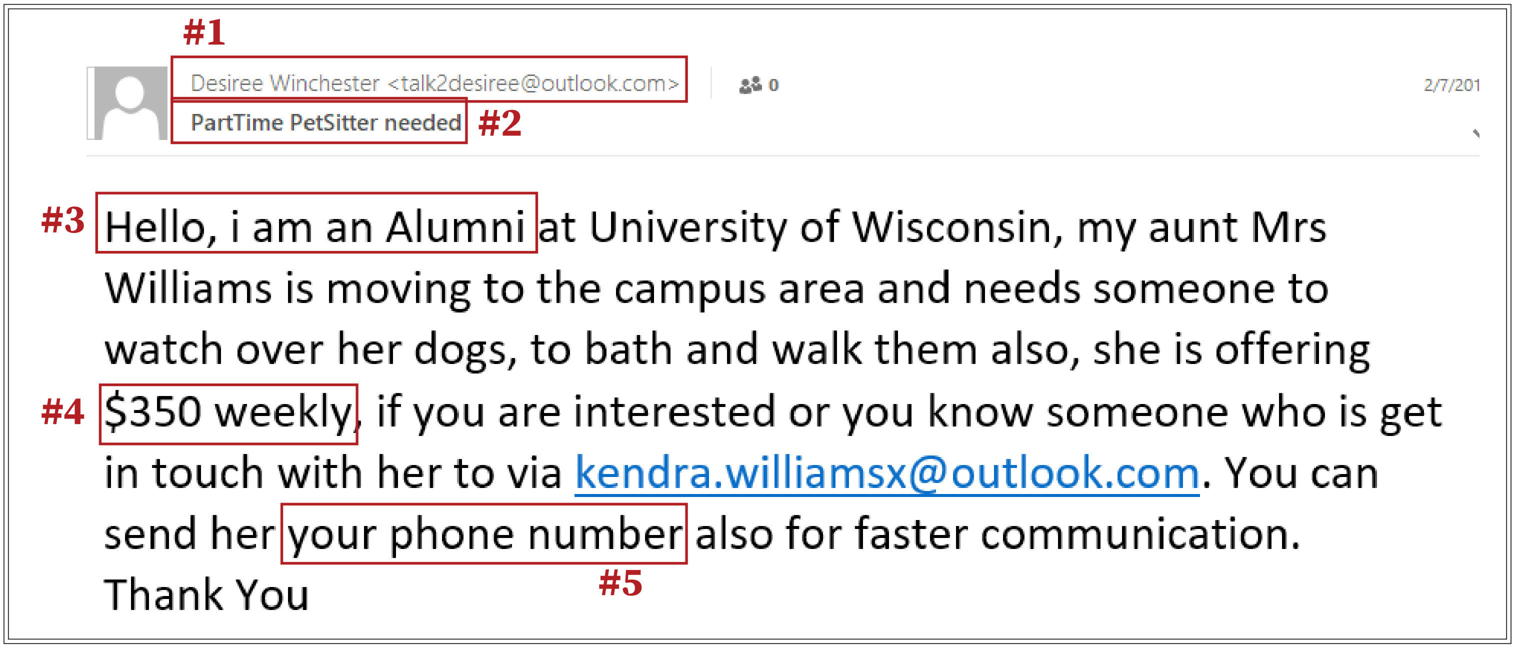
University of Wisconsin
Whitewater

Instructional Communication
and Information Technology

Spot That Phish!

Phishing is a form of fraud where a cyber-criminal attempts to lure you into revealing your personal, financial or confidential information by impersonating a trusted source through electronic communication.

Below are examples of phishing scams sent to UW-W this year. We have pointed out some of the characteristics that can help you spot a phish.



Desiree Winchester <talk2desiree@outlook.com>

2/7/201

PartTime PetSitter needed

Hello, i am an Alumni at University of Wisconsin, my aunt Mrs Williams is moving to the campus area and needs someone to watch over her dogs, to bath and walk them also, she is offering $350 weekly, if you are interested or you know someone who is get in touch with her to via kendra.williamsx@outlook.com. You can send her your phone number also for faster communication.
Thank You

Here’s what we found to be suspicious:

#1: The email is coming from an outside source (not a UW-W or UW email address).
- If you do not see the email address, hover over the sender’s name to see their email.

#2: The subject of the email has grammar and capitalization inconsistencies.
- Take the time to look for this. Would a supervisor make these kind of mistakes?

#3: The greeting is generic, the “i” is lowercase, and they present a vague identity.
- They sender does not identify themselves in the email, nor do they greet you specifically.

#4: The offer seems a bit too good to be true, considering the work.
- Do the math, does this seem like a fair wage for the type of work? Usually the offer of money is a red flag.

#5: The sender is asking for your personal information.
- Once they have your info you are at risk of identify/financial theft, or will continue to be targeted by future scams.