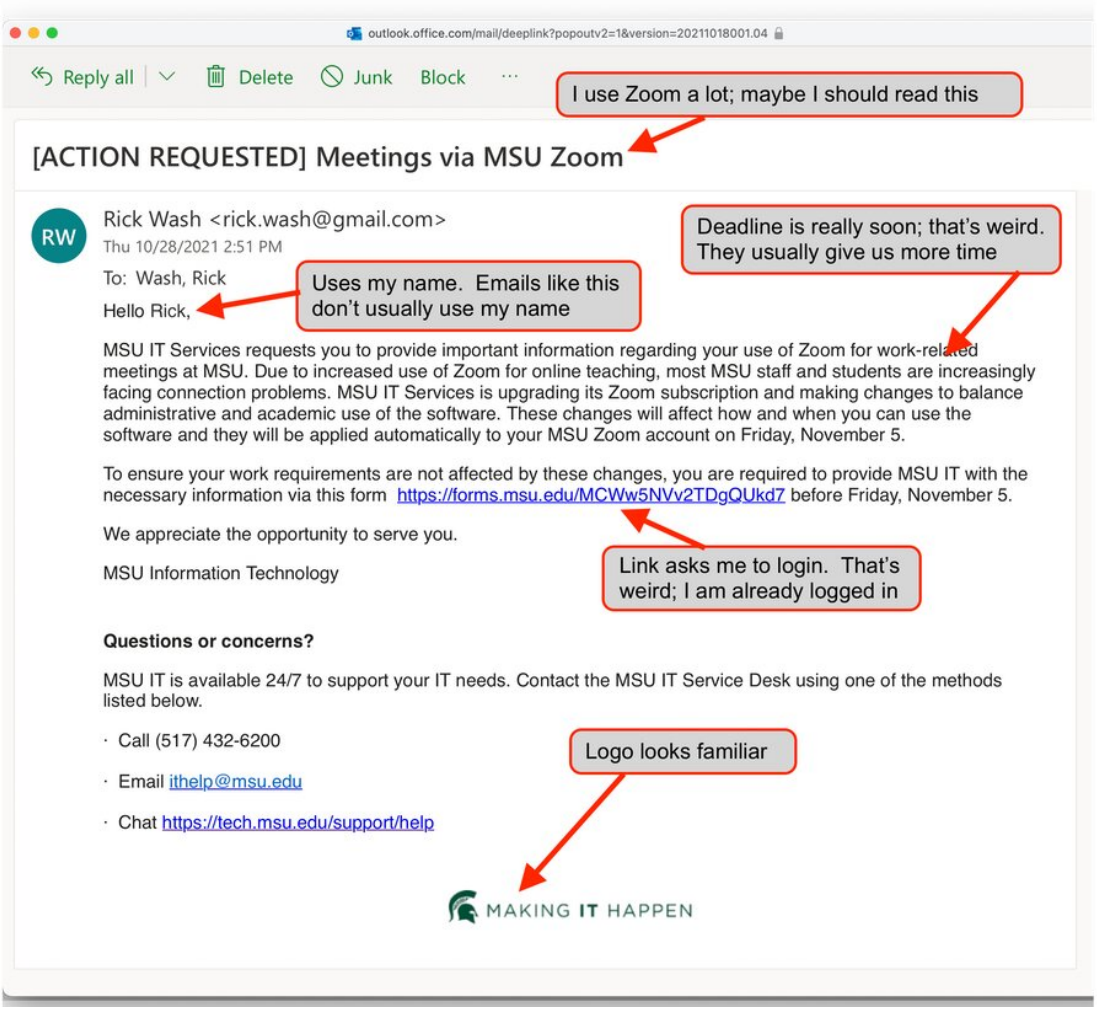
How to trust your instincts to foil phishing attacks

November 2 2021, by Rick Wash



Aspects of an email message that seem off should prompt you to consider the possibility of phishing. The trick is remembering that phishing exists. Credit: Rick Wash, CC BY-ND 4.0

An employee at MacEwan University got an email in 2017 from someone claiming to be a construction contractor asking to change the account number where almost $12 million in payments were sent. A week later the actual contractor called asking when the payment would arrive. The email about the account number change was fake. Instead of going to the contractor, the payments were sent to accounts controlled by criminals.

Fake emails that try to get people to do things they wouldn't normally do, such as send money, run dangerous programs or give out passwords, are known as phishing emails. Cybersecurity experts often blame the people who receive such messages for not noticing that the emails are fake.

As a cybersecurity researcher, I've found that most people are good at almost all of the skills that computer security experts use to notice fake emails in their inboxes. Making up the difference comes down to listening to your instincts.

How the pros do it

In earlier research, I found that when cybersecurity experts received a phishing email message, they, like most people, assumed the email was real. They initially took everything in the email at face value. They tried to figure out what the email was asking them to do, and how it related to things in their life.

As they read, they noticed small things that seemed off, or different from what would typically be in similar email messages. They noticed things like typos in a professional email, or the lack of typos from a busy executive. They noticed things like a bank providing account information in an email message instead of the standard notification that the recipient had a message waiting for them in the bank's secure messaging system. They also noticed things like someone

uncharacteristically emailing them without mentioning it in person first.

But noticing these signs isn't enough to figure out the email is a fraud. Instead, the experts just became uncomfortable with the email message. It wasn't until they saw something in the message that reminded them of phishing that they became suspicious. They would see an anomaly like a link that the email was trying to get them to click. In their minds, these are commonly associated with phishing emails.

Combined with the uncomfortable feeling about the email message, this reminder prompted the experts to recognize that phishing might explain the weird things they noticed. They became suspicious of the message and investigated to figure out if it was a fraud.

Good instincts

If that's how experts do it, then what do regular people do? When I interviewed people without computer security experience, I found a similar process. Most people noticed things that seemed off, became uncomfortable with the email, remembered about phishing and investigated.

My research found that people are good at the first two steps: noticing things in the email that seem weird, and becoming uncomfortable. Almost everyone I talked to noticed multiple problems when they saw a fake email, and told me about feeling uncomfortable with the message.

And if people thought about phishing, they were also good at investigating. Instead of looking at technical details, though, most people either contacted the sender or asked others for help. But they were still able to correctly figure out whether an email message was a phishing attack.

Phishing stories

Most phishing training teaches people to look for problems in email. But for most people, the hard part about phishing isn't noticing the weird things in an email message. People often deal with weird but real emails. Many messages feel a little bit off. Sometimes your boss is having a bad day, or the bank changes its polices. No email message is perfect, and people are often attuned to that.

The challenge for most people was remembering that phishing exists, and recognizing that phishing might explain those weird things. Without that awareness of phishing, the weirdness in phishing messages can be lost in everyday email weirdness.

Most people I interviewed know about phishing in general. But the people who were good at noticing phishing messages reported stories about specific phishing incidents they had heard about. They told me about a time when someone at their organization fell for a phishing email, or about a news story of an incident like the one at MacEwan University.

Familiarity with specific phishing incidents helps people remember phishing generally and recognize that it might explain the weird things they notice in an email. These stories are key to people going from "something's fishy" to "is this phishing?"

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: How to trust your instincts to foil phishing attacks (2021, November 2) retrieved 19

April 2024 from https://techxplore.com/news/2021-11-instincts-foil-phishing.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.