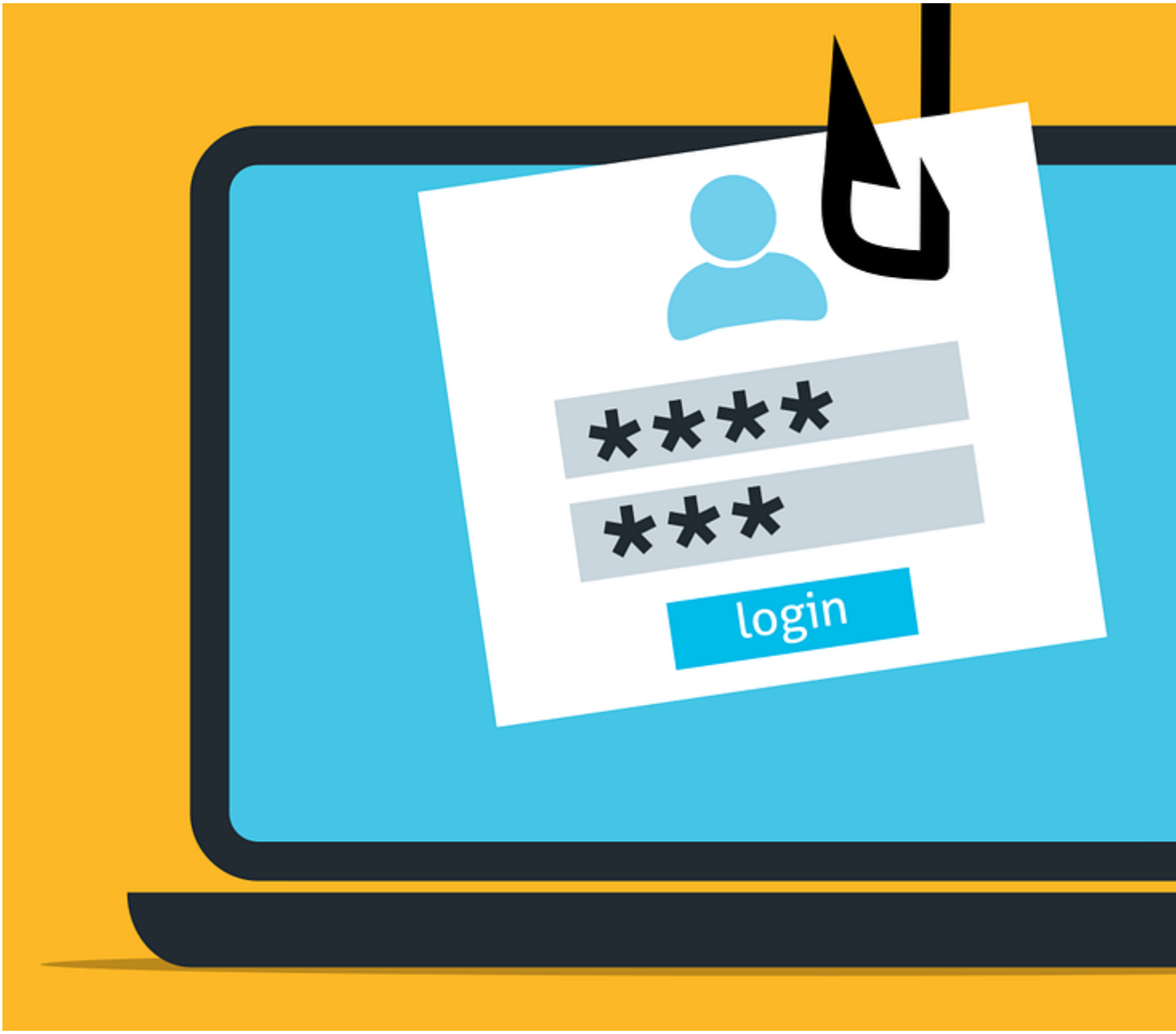
Published on *University of Colorado* (https://www.cu.edu)



# Fight the Phish [1]




The cybersecurity space has been as hectic as it has ever been over the last 12 to 24 months. However, for all the emerging threats and news that are cropping up on the horizon, phishing—one of the oldest pain points in cybersecurity – continues to be a threat to individuals and organizations.

According to Verizon's Data Breach Investigation Report, 43 percent of cyberattacks in 2020 featured phishing or pre-texting, while 74 percent of US organizations experienced a successful phishing breach last year alone. That means that phishing scams continue to

impact an organization’s cybersecurity health.

With that in mind, here are a few quick best practices and tips for dealing with phishing threats.

**Know the Red Flags**

Cybercriminals are masters of making their phishing content and interactions appealing. From content design to language, it can be difficult to discern whether content is genuine or a potential threat, which is why it is so important to know the red flags. Awkward and unusual formatting, overly explicit call outs to click a hyperlink or open an attachment and subject lines that create a sense of urgency are all hallmarks that the content you received could be potentially from phish and indicate that it should be handled with caution.

**Verify the Source**

Phishing content comes in a variety of ways, however, many phishes will try to impersonate someone you may already know -- such as a colleague, service provider or friend -- as a way to trick you into believing their malicious content is actually trustworthy. Don’t fall for it. If you sense any red flags that something may be out of place or unusual, reach out directly to the individual to confirm whether the content is authentic and safe. If not, break-off communication immediately and flag the incident through the proper channels.

**Be Aware of Vishing and Other Phishing Offshoots**

As more digital natives have come online and greater awareness has been spread about phishing, bad actors have begun to diversify their phishing efforts beyond traditional email. For example, voice phishing -- or vishing -- has become a primary alternative for bad actors looking to gain sensitive information from unsuspecting individuals. Similar to conventional phishing, vishing is typically executed by individuals posing as a legitimate organization -- such as a healthcare provider or insurer -- and asking for sensitive information. Simply put, it is imperative that individuals be wary of any sort of communication that asks for personal information whether it be via email, phone or chat -- especially if the communication is unexpected. If anything seems suspicious, again, break-off the interaction immediately and contact the company directly to confirm the veracity of the communications.

**Remember...**

Phishing may be “one of the oldest tricks in the book,” but it is still incredibly effective. And although it may be hard to spot when you may be in the midst of a phishing attempt, by exercising caution and deploying these few fundamentals, individuals and organizations can mitigate the chances of falling victim to a phishing attack.

**Learn more**

- Phishing Scams FAQs [2]
- Roger Grimes, Data Driven Defense Evangelist, KnowBe4, Inc. "Fight the Phish" Webinar Recording [3] (PowerPoint presentation is provided below.)

**Attachments:**
22 Red Flags [4]
Red Flags of Rogue URLS [5]

Roger Grimes PowerPoint Presentation "Fight the Phish" [6]

**Groups audience:**

Office of Information Security

---

**Source URL:** https://www.cu.edu/security/fight-phish

**Links**

[1] https://www.cu.edu/security/fight-phish
[2] https://www.cu.edu/security/awareness/phishing-scams-faqs
[3] https://cuboulder.zoom.us/rec/share/9mhVk8eiAhvfiezbZg8ZxqMzPJUDZxViKwz-S3LyXNib7HmPLgImFK-YCGZjM-ii.69WIE1RaCQBmsUG4
[4] https://www.cu.edu/doc/22redflagspdf
[5] https://www.cu.edu/doc/red-flags-rogue-urlspdf
[6] https://www.cu.edu/doc/kb4-fightthephish25pdf