

Protect Against Phishing Attempts

Via Ultipro

As COVID-19 continues to impact us all, there has been an unfortunate increase in scams related to the global pandemic reported around the world. Because safeguarding you and your people is of utmost importance to us, we want to share some steps you can take to protect your organization right now. Please take a few minutes to educate yourself and your employees on the dangers of phishing.

What is phishing?

- It's an electronic communication—like email or text messages (SMS)—that attempts to obtain personal data, such as usernames, passwords, and more, for malicious reasons.
- The communication is disguised to look like it's coming from a trustworthy source. Unfortunately, phishing attempts can appear legitimate by incorporating company brands, names, and colors.
- Phishing emails often contain links to websites that may ask you to submit your personal information and/or download virus-infected programs.

We encourage you to take proactive steps to protect your important information. To get started, reach out to your in-house IT department and work together to guard against phishing attempts. If you receive an email that you suspect may not be legitimate, it is very important that you:

- Do not respond to the email.
- Do not click on any links in the email.
- Do not open any suspicious email attachments.
- Do not provide any data to websites or individuals as a result of the email.

In response to COVID-19, it's important to remain especially vigilant of requests for financial information either via email or phone. **Always verbally confirm any requested change in banking information or a request to re-route any electronic payments.** For more information about COVID-19 scams, [read this alert](#) from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In addition, you can

read COVID-19 consumer warnings and safety tips from the Federal Communications Commission (FCC) [here](#).

We also invite you to leverage the many security features UltiPro® makes available to you. When enabled, tools like multifactor authentication can help provide additional layers of security beyond your username and password. To learn more, head to the Learning Center in the Customer Success Portal and find more information about UltiPro's robust security offerings under *Content > System Management > Security*.

If you suspect someone is fraudulently claiming to be Ultimate Software, please contact us right away via security@ultimatesoftware.com.