As your organization’s security awareness officer or as part of your security team, you may be asked what your organization should be communicating to your workforce during these unprecedented times. Below you will find a template that can be customized to the needs of your organization. The links below go directly to [OUCH! Security Awareness newsletters](https://sans.org/ouch) that go into more information on each topic. Each newsletter is translated into over 25 languages so should be accessible for any workforce. In many ways, people are scared. As such, our job as security professionals, is to keep our communications calm, simple and actionable.

*With recent events in the news, we know you have questions and concerns. One of those may be about cybersecurity. Am I, or is our company, more likely to come under attack? Am I at greater risk? We don’t have all the answers, nor do we know what will happen next. But we do know from a cybersecurity perspective, continue to focus on the fundamentals, that is key to protecting both yourself at home and at work. While the sense of urgency may have changed, how cyber attackers target us has not. By fundamentals, we mean focus on these three key points.*

1. [***Phishing***](https://www.sans.org/newsletters/ouch/social-engineering-attacks/)*: Phishing and related scams are when cyber attackers attempt to trick or fool you into doing something you should not do. Often these scams are sent as emails, but they can also try to trick with you text messaging, phone calls or on social media. Anytime someone is creating a tremendous sense of urgency and rushing you to take an action, or someone is promoting an offer that is too good to be true, this is most likely an attack.*
2. [***Passwords***](https://www.sans.org/newsletters/ouch/making-passwords-simple/)*: Strong passwords are the key to protecting your online, digital life. Make sure each of your accounts is protected by a unique, long password. The longer your password the better. To keep it simple, use passphrases, a type of password made up multiple words like “honey-butter-happy”. Can’t remember all your passwords? Neither can we. That is why we also recommend you use a Password Manager to securely store all your passwords. Finally, whenever possible, enable Multi-Factor Authentication (MFA) on your important accounts.*
3. [***Updating***](https://www.sans.org/newsletters/ouch/the-power-of-updating/)*: Keep your computers, devices and apps updated and current by enabling automatic updating on all your devices. Cyber attackers are constantly looking for new vulnerabilities in the devices and software you use. Keeping them automatically updated makes sure these known weaknesses are fixed and your devices have the latest security features.*

*In addition, there is going to be a tremendous amount of* [*false information*](https://www.sans.org/newsletters/ouch/fake-news/) *spread on the Internet. This is being done by the Russian government on purpose to confuse people. Do not trust or rely on information from new, unknown or random social media accounts, such as posts on LinkedIn, Instagram, Facebook or Twitter. Many accounts on these sites were created for the sole purpose of putting out fake information. Instead, follow only well-known trusted news sources who verify the authenticity of information before they broadcast it. Finally, if you wish to donate to any causes in support of recent events, once again make sure you are donating to a well-known, trusted charity. There will be many scams attempting to trick people into donating to fake charities ran by cyber criminals.*

*We know that times like these can feel a bit scary, but we also wanted to let you know you will be fine. Continue to focus on the fundamentals as we have taught you, and you will go a long way to protecting yourself, no matter who the cyber attacker is.*

Savvy threat actors are going to try their best to capitalize upon the anxiety, fear, and emotion many of us will be dealing with during uncertain times. Prompt and clear communication is a key first step to navigating through these situations safely.