Якщо ви керівник із питань безпеки вашої організації або співробітник відділу з питань безпеки, вас можуть запитати, як ваша організація має спілкуватися зі своїми співробітниками в ці безпрецедентні часи. Нижче ви знайдете шаблон, який можна налаштувати відповідно до потреб вашої організації. Нижченаведені посилання спрямовують безпосередньо до документів: [OUCH! Інформаційні бюлетені з питань безпеки](https://sans.org/ouch), які містять більше інформації з кожної теми. Кожний інформаційний бюлетень перекладено більше ніж 25 мовами, тому з ним може ознайомитися співробітник будь-якого трудового колективу. У багатьох відношеннях люди налякані. Таким чином, наша робота як професіоналів у сфері безпеки полягає в тому, щоб забезпечувати спокійне, легке й дієве спілкування.

*З огляду на останні події в новинах, ми знаємо, що у вас є запитання й побоювання. Одне з них може стосуватися кібербезпеки. «А чи, швидше за все, підпаду під удар я чи наша компанія?» «Чи піддаюся я більшому ризику?» Ми не маємо відповідей на всі ці запитання, і ми не знаємо, що буде далі. Але нам точно відомо, з точки зору кібербезпеки, що необхідно продовжувати зосереджуватися на основних принципах, які є ключовими для захисту себе як вдома, так і на роботі. Хоча відчуття невідкладності, можливо, змінилося, спосіб, яким кіберзловмисники націлюються на нас, залишився тим самим. Під принципами ми маємо на увазі зосередженість на трьох нижченаведених ключових моментах.*

1. [***Фішинг***](https://www.sans.org/newsletters/ouch/social-engineering-attacks/)*. Фішинг і пов’язані з ним шахрайства — це ситуація, коли кібер-зловмисники намагаються обхитрити або обдурити вас з метою спонукати зробити дії, які вам не слід робити. Часто такі фішингові повідомлення надсилаються у вигляді електронних листів, але зловмисники можуть також спробувати вас обдурити за допомогою текстових повідомлень, телефонних дзвінків або соціальних мережах. Щоразу, коли хтось створює неймовірне відчуття невідкладності та вас кваплять вжити заходів, або хтось просуває пропозицію, занадто гарну, щоб бути правдою, це, швидше за все, атака.*
2. [***Паролі***](https://www.sans.org/newsletters/ouch/making-passwords-simple/)*. Наявність надійних паролів є ключовою умовою захисту вашого життя в цифровому світі в онлайн режимі. Переконайтеся, що кожен з ваших облікових записів захищений унікальним довгим паролем. Чим довший ваш пароль, тим краще. Щоб було простіше, використовуйте фрази-паролі, тобто типи паролів, що складаються з кількох слів, наприклад «honey-butter-happy». Не можете запам’ятати всі свої паролі? Ми також не можемо. Тому, щоб безпечно зберігати всі свої паролі, рекомендуємо також використовувати диспетчер паролів. Нарешті, якщо це можливо, увімкніть багатофакторну автентифікацію (MFA) у ваших важливих облікових записах.*
3. [***Оновлення***](https://www.sans.org/newsletters/ouch/the-power-of-updating/)*. Оновлюйте свої комп’ютери, пристрої та програми, увімкнувши автоматичне оновлення на всіх своїх пристроях. Кіберзловмисники постійно шукають нові вразливі місця в пристроях і програмному забезпеченні, які ви використовуєте. Їх автоматичне оновлення гарантує, що ці відомі недоліки буде виправлено, а ваші пристрої отримають найновіші функції безпеки.*

*Додатково очікується, що через Інтернет буде розповсюджуватися величезна кількість*[*неправдивої інформації*](https://www.sans.org/newsletters/ouch/fake-news/)*. Це робиться російським урядом навмисне, щоб заплутати людей. Не довіряйте й не покладайтеся на інформацію з нових, невідомих або випадкових облікових записів у соціальних мережах, як-от: публікацій в LinkedIn, Instagram, Facebook або Twitter. Багато облікових записів на цих сайтах були створені з єдиною метою розповсюдження фейкової інформації. Замість цього слідкуйте лише за відомими надійними джерелами новин, які перевіряють достовірність інформації, перш ніж поширювати її.*

*Нарешті, якщо ви бажаєте зробити пожертви на будь-які цілі для підтримки останніх подій, ще раз переконайтеся, що ви робите пожертвування відомій, надійній благодійній організації. Існує багато шахраїв, які намагатимуться обманом змусити людей зробити пожертви для фальшивих благодійних організацій, якими керують кіберзлочинці.*

*Нам відомо, що в такі часи трохи страшно, але ми також хотіли вам повідомити, що у вас все буде добре. Продовжуйте зосереджуватися на основних принципах, яким ми вас навчили, і ви зможете захистити себе, незалежно від того, хто є кіберзловмисником.*

Розумні суб’єкти загрози намагатимуться зробити все можливе, щоб отримати вигоду із занепокоєння, страху та емоцій, з якими багато з нас будуть мати справу в часи нестабільності. Швидке та чітке спілкування є ключовим першим кроком до безпечного подолання цих ситуацій.