Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Водич за сајбер безбедност за мали бизниси

Сложеност на содржината
ЕДНОСТАВНА ● ○ ○

cyber.gov.au

Вовед

За мал бизнис, дури и мал инцидент во врска со сајбер безбедноста може да има катастрофални последици. Овој водич ги вклучува основните безбедносни мерки за да ви помогнат да го заштитите вашиот бизнис од вообичените закани по сајбер безбедноста. За почеток, ви ги преопрачуваме следните три мерки:

- **Вклучете ја мулти-фактор автентикацијата**
- **Ажурирајте го вашиот софтвер**
- **Правете резервни копии на вашите податоци**

Овој водич може да содржи мерки кои не се соодветни за вашиот бизнис или можеби вашиот бизнис има посложени потреби. Откако ќе ги спроведете мерките од овој водич, им препорачуваме на малите бизниси да го воспостават Првото ниво на компетенција (Maturity Level One) од Неопходните осум (Essential Eight). Ако имате прашања во врска со овие совети или сајбер безбедноста пошироко, ви препорачуваме да разговарате со ИТ професионалец или советник на кој му верувате.

Посетете ја веб-страницата cyber.gov.au за да го прочитате водичот во целост, вклучувајќи практични совети за секоја мерка.

Содржина

Закани за малите бизниси

Лажни пораки

Лажните пораки се вообичаен начин што го користат сајбер криминалците за да ги имаат на мета малите бизниси. Нивната цел е да ве измамат вас или вашиот персонал:

- да испратите пари или подарок-картички
- да кликнете на злонамерни линкови или прилози
- да дадете чувствителни податоци, на пример, лозинки.

Сајбер криминалците може да се обидат и да го измамат вашиот бизнис преку имејл, текстуални пораки, телефонски повици и социјални мрежи. Тие често ќе се преправаат дека се лице или организација на кои им верувате.

Напади преку лажно претставување

На малите бизниси посебна загриженост им создаваат **нападите преку лажно претставување (phishing attacks)**. Овие лажни пораки често содржат линк до лажна веб-страница на која ве наведуваат да се најавите на сметка или да внесете доверливи податоци.

Нападите преку лажно претставување обично ги компромитираат лозинките на вашите сметки. Сајбер криминалците често го користат овој метод за да ги „преземат" сметките на малите бизниси на социјалните мрежи и да ги чуваат за уценување.

Начини за намалување на инциденти

Ако пораката е од познат субјект и ви изгледа сомнителна, бидете внимателни. Контактирајте го лицето или бизнисот одделно за да проверите дали пораката е легитимна. Користете ги контактните податоци што ќе ги најдете преку легитимен извор, на пример, посетете ја официјалната веб-страница на бизнисот, а не оние кои се наоѓаат во сомнителната порака.

Дознајте повеќе како да идентификувате лажни пораки и напади со лажно претставување во следните материјали:

- Препознавајте и пријавувајте лажни пораки
- Научете како да забележите измами со лажно претставување
- Откривање на пораки од социјален инженеринг.

Студија на случај:

Службеничка во компанија за курирски услуги доби имејл од еден од управниците, со барање да купи 6 однапред платени кредитни картички Mastercard од 500 долари. Управникот ѝ рече да го чува тоа во тајност бидејќи картичките ќе бидат подарок-ваучери за членови од персоналот. На службеничката ѝ беше кажано откако ќе ги купи картичките да ги фотографира двете страни од картичките како доказ дека ги купила.

Според упатствата, службеничката отиде во пошта и ја употреби својата лична кредитна картичка за да ги купи подарок-картичките. Таа одговори на имејлот на управникот и испрати фотографии од подарок-картичките како доказ.

По враќањето од пошта, службеничката му ги даде физичките картички на управникот - кој не знаеше за нив. По прегледот **на сите имејли во врска со подарок-картичките, беше утврдено дека тие пристигнале од случајна имејл адреса и не беа од легитимната имејл сметка на управникот. Тоа беше измама.**

Напади со имејл

Покрај измамите како што е лажно претставување, вообичаен напад на малите бизниси со имејл е **компромитирање на деловен имејл (business email compromise**) (BEC). Криминалците можат да имитираат деловни претставници со користење на компромитирани имејл сметки или на други начини - како на пример со користење на име на домен што изгледа слично на вистински бизнис. Покрај кражба на податоци, целта на овие напади обично е да ги измамат жртвите да испратат средства на банкарска сметка со која управува измамникот.

Начини за намалување на инциденти

Најдобрата одбрана е обука и запознавање на вашите вработени за напади со имејл. Погрижете се вашиот персонал да знае дека секогаш треба да биде претпазлив со имелји што го содржат следното:

- барања за исплата, посебно ако се итни или доцнат
- промена на банкарски податоци
- имејл адреса што не изгледа сосема во ред, на пример, името на доменот не се совпаѓа целосно со името на компанијата на добавувачот.

Иако овие напади можат да бидат катастрофални, мерките за намалување на инциденти се лесни и не чинат речиси ништо. **Кога персоналот добива вакви имејли, најефикасно е да го повикате испраќачот за да потврдите дека тој е легитимен.** Не користете ги податоците за контакт што ви се испратени, бидејќи тие може да бидат лажни. Воведете формален процес што персоналот треба да го следи кога се примаат барања за исплата или се менуваат банкарски податоци.

Дознајте повеќе како да го заштитите вашиот бизнис од BEC-измами и компромитирани имејли со следните материјали:

- Компромитирање на деловен имејл
- Заштитете го вашиот бизнис од лажни и компромитирани имејли
- Што треба да правите ако вашиот бизнис е мета на лажни или компромитирани имејли.

Студија на случај:

Мала градежна компанија доби имејл од нејзиниот добавувач во која се вели дека ја смениле банката. Добавувачот ги достави податоците на новата сметка за плаќање на фактури. Бидејќи имејлот изгледаше легитимен, **градежната компанија не му се јави на добавувачот за да ја потврди промената на податоците на банкарската сметка.**

Компанијата плати фактура од добавувачот во износ од 70.000 долари. Следниот ден, друг вработен по грешка повторно ја плати истата фактура во дополнителен износ од 70.000 долари. Вкупно, на новата банкарска сметка беа исплатени над 150.000 долари.

Кога компанијата се јави на нивниот добавувач за да праша дали може да им се врати извршената двојна исплата, добавувачот им кажа дека тие банкарски податоци се неточни. Веднаш беше спроведена истрага и добавувачот откри дека една од нивните имејл сметки била хакирана и од неа биле испратени податоците за лажната банкарска сметка. **Средствата не беа вратени.**

Злонамерен софтвер

Злонамерен софтвер Malware е општ термин кој се користи да се опише злобен софтвер дизајниран да предизвика штета, како на пример, уценувачки програми, вируси, шпионски софтвер и тројански коњи. Злонамерниот софтвер може:

- да краде или заклучува датотеки на вашиот уред
- да ги украде броевите на вашите банкарски или кредитни картички
- да ги украде вашите кориснички имиња и лозинки
- да преземе контрола или да шпионира на вашиот компјутер.

Злонамерниот софтвер може да го спречи вашиот уред да работи правилно, да ги избрише или оштети вашите датотеки, или да им дозволи на други да имаат пристап до вашите лични или деловни податоци. Ако вашиот уред е заразен со злонамерен софтвер, може да бидете ранливи на други напади. Злонамерниот софтвер може да се прошири и на други уреди на вашата мрежа.

Вашиот уред може да биде заразен со злонамерен софтвер на повеќе начини, вклучително со:

- посетување на веб-страници што се заразени со злонамерен софтвер
- преземање на заразени датотеки или софтвер од интернет
- отварање на заразени прилози во имејл.

Уценувачки програми

Уценувачките програми (ransomware) се вообичаен и опасен вид на злонамерен софтвер. Работат така што ги заклучуваат или шифрираат вашите датотеки за да не можете повеќе да им пристапувате. За да се врати пристапот до датотеките се бара плаќање на откуп, обично во форма на криптовалута. Сајбер криминалците може исто така да се закануваат дека ќе ги објават или продадат податоците онлајн, освен ако не се плати откуп.

Начини за намалување на инциденти

Иако антивирусен или безбедносен софтвер може да помогне да се заштитите од злонамерен софтвер, не постои софтвер кој е 100% ефикасен. Персоналот мора да биде претпазлив со имејли, веб-страници и преземање на датотеки, како и редовно да ги ажурира уредите за да бидат безбедни.

Видете г следните материјали за повеќе информации како да го заштитите вашиот бизнис од уценувачки програми:

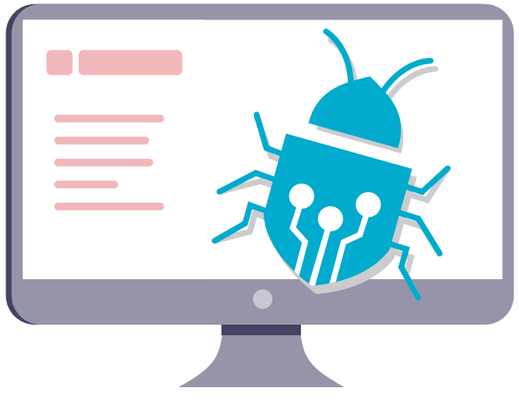
- Уценувачки програми
- Заштитете се од напади со уценувачки програми
- Што треба да направите ако сте заложник.

Студија на случај:

Вработените во продавница за автоделови дојдоа на работа едно утро и не можеа да го стартираат серверот. Кога нивниот испорачувач на ИТ услуги доби пристап до серверот, најде отворен прозорец на кој пишуваше дека сите комјутерски податоци се шифрирани. Во белешката се бараше тие да платат откуп во биткоини за да се отклучат датотеките.

На компјутерот беше приклучен резервен диск, на кој податоците исто така беа шифрирани. **Тие се обидоа да поврзат повеќе резервни дискови, меѓутоа датотеките беа автоматски шифрирани за неколку секунди. Тие не успееја да ја отстранат уценувачката програма пред да се обидат да ги вратат нивните податоци и ги изгубија сите резервни датотеки што ги имаа.**

Единствената опција што остана беше фабрички да се ресетира серверот и да се започне одново со нов систем. Нивниот бизнис изгуби податоци од многу години и мораше да започне одново.



Заштитете ги вашите сметки

Вклучете ја мулти-фактор автентикацијата

Мулти-фактор автентикацијата (MFA) им отежнува на сајбер криминалците да добијат пристап до вашите сметки.

Таа додава уште еден слој на безбеност на вашата сметка. Таа е еден од најефикасните начини да ги заштитите вашите сметки од некој да добие пристап, па затоа треба да ја користите секогаш кога е можно. Секој што ќе се најави на вашата сметка ќе биде обврзан да стави нешто друго покрај вашето корисничко име и лозинка. Ова може да биде единствена шифра од текстуална порака или апликација за автентикатор. За повеќе информации, прочитајте ги нашите совети за MF, достапни на **cyber.gov.au/mfa.**

✓ **Вклучете ја MFA секогаш кога тоа е можно, започнувајќи со вашите најважни сметки.**

Воспоставете контрола на пристап

Ограничувањето на пристап за корисници може да ја ограничи штетата предизвикана од инцидент во врска со сајбер безбедноста.

Контролата на пристап е начин на ограничување на пристапот до одредени датотеки и системи. Вообичаено, на персоналот не му е потребен целосен пристап до сите податоци, сметки и системи во бизнисот. Треба да им се дозволи пристап само до она што им е потребно за извршување на нивните должности.

Ограничувањето на пристапот ќе помогне да се ограничи штетата предизвикана од инцидент во врска со сајбер-безбедноста. На пример, ако компјутерот на член на персоналот е заразен со уценувачка програма, со соодветни контроли таа може да влијае само на мал број датотеки, а не на целиот бизнис.

✓ **Погрижете се секој корисник да има пристап само до тоа што му е потребно за неговата работа.**

Користете сигурни лозинки или лозинки во форма на фрази

Заштитете ги вашите сметки од сајбер криминалци со безбедна лозинка или лозинка во форма на фраза.

Многу мали бизниси се соочуваат со сајбер напади како резултат на лошо користење на лозинки. На пример, повторно користење на иста лозинка на повеќе сметки. Можете исто така да користите „управувачи на лозинки“ (password managers) и лозинки во форма на фрази за да креирате сигурни лозинки.

„Управувачот на лозинки“ делува како виртуелен сеф за вашите лозинки. Можете да го користите за да креирате и чувате сигурни и единствени лозинки за секоја од вашите сметки. Ако имате многу сметки, ова ја отстранува обврската да памтите **единствени** лозинки. Не мора да ги запомнувате лозинките или сметките на кои тие припаѓаат, бидејќи сè е запишано во вашиот „управувач на лозинки“.

За сметките на кои редовно се најавувате или кои не сакате да ги чувате во „управувачот на лозинки“, размислете да користите лозинка во форма на фраза. Лозинките во форма на фраза се комбинација од случајни зборови, на пр. „глинен перек со кристален кромид“. Тие се корисни кога сакате сигурна лозинка која е лесна за паметење. Користете случајна комбинација од четири или повеќе зборови и чувајте ја единствена - **не користете повторно лозинка** во форма на фраза за повеќе сметки. За повеќе информации, прочитајте ги нашите совети за лозинки во форма на фрази и управувачи на лозинки, достапни на **cyber.gov.au/passphrases.**

✓ **Користете „управувач на лозинки“ за да креирате и чувате единствени лозинки за секоја од вашите важни сметки.**

Управувајте со заеднички сметки

Споделувањето на сметки може да ја загрози безбедноста и да го отежни следењето на злонамерна активност.

Во мал бизнис, може да има легитимни причини зошто персоналот треба да споделува сметки, но тоа треба да се избегнува колку што е можно повеќе. Кога повеќе вработени користат иста сметка, може да биде тешко да се следи активноста на одредено вработено лице и уште потешко да се следат сајбер криминалците кои влегле насилно. Освен ако не ја промените лозинката, вработените може да продолжат да пристапуваат до сметките дури и откако ќе го напуштите бизнисот.

✓ **Ограничете го користењето на заеднички сметки и заштитете ги оние што се користат во вашиот бизнис.**

Заштитете ги вашите уреди и податоци

Ажурирајте го вашиот софтвер

Ажурирањето на софтверот е еден од најдобрите начини да го заштитите вашиот бизнис од сајбер напади.

Со ажурирање може да ги поправите безбедносните пропусти во вашиот оперативен систем и другиот софтвер, со што ќе се отежне влегување на сајбер-криминалец. Постојано се откриваат нови грешки, затоа не ги игнорирајте барањата за ажурирање. Редовното ажурирање на софтверот ќе ја намали можноста сајбер-криминалецот да користи позната слабост за да стартува малициозен софтвер или да го хакира вашиот уред. Ако ви треба помош, ACSC објави упатства за ажурирање.

Ако вашиот уред или софтвер е премногу стар, можеби ажурирањето нема да биде достапно. Ако производителот престанал да го поддржува производот со ажурирање, размислете за надградба на понов производ за да останете безбедни. Примери на системи кои повеќе не добиваат важно ажурирање се **iPhone 7** и **Microsoft Windows 7**.

За повеќе информации, прочитајте ги нашите упатства за ажурирање, достапни на **cyber.gov.au/updates.**

Вклучете го автоматското ажурирање за вашите уреди и софтвер.

Користете безбедносен софтвер

Безбедносниот софтвер како што се заштита од антивируси и уценувачки програми може да помогне да ги заштитите вашите уреди.

Користете безбедносен софтвер за откривање и отстранување на злонамерен софтвер од вашите уреди. Антивирусниот софтвер може да се постави редовно да скенира за сомнителни датотеки и програми. Кога ќе се открие закана, ќе добиете предупредување и сомнителната датотека ќе биде ставена во карантин или избришана.

Многу мали бизниси можат да користат „Windows Security“ за да се заштитат од вируси и злонамерен софтвер. **„Windows Security“** е вграден во уредите со Windows 10 и Windows 11 и вклучува бесплатна заштита од вируси и закани. Може да го користите и за да ги вклучите функциите на вашиот уред за заштита од уценувачки програми.

За алтернативни производи и опции, прочитајте ги нашите совети за антивирусен софтвер, ако пребарате *„antivirus“* на cyber.gov.au.

Поставете безбедносен софтвер на вашите уреди за да прави редовно скенирање.

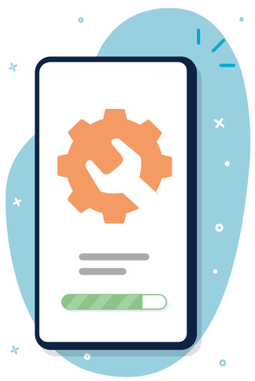
Правете резервни копии на вашите податоци

Редовното правење резервни копии на вашите податоци може да ви помогне да ги обновите ако се загубени или компромитирани.

Правењето резервна копија на важни податоци треба да биде редовна или автоматска пракса во вашиот бизнис. Без редовно правење на резервни копии, би можело да биде невозможно да ги повратите вашите податоци по сајбер напад.

Постојат многу методи и производи што можете да ги користите за да направите резервна копија на вашите податоци. За детални совети за правење резервни копии на податоци во вашиот бизнис, прочитајте ги нашите совети за правење резервни копии на податоци, достапни на **cyber.gov.au/backups**. Најдобрата опција за секоја компанија ќе биде различна, затоа разговарајте со ИТ професионалец ако не сте сигурни.

Направете и спроведете план редовно да правите резервни копии од вашите податоци.



Заштитете ја вашата мрежа и надворешните услуги

Заштитете го вашиот бизнис од сајбер напади со отстранување на потенцијалните пропусти во вашата мрежа.

Уредите и услугите на вашата мрежа може да бидат главна мета за сајбер криминалците. Многу од овие системи може да бидат сложени за да се заштитат, затоа ве молиме разговарајте за следните препораки со ИТ професионалец.

- **Заштитете ги вашите сервери:** Ако користите NAS или друг сервер во вашиот дом или бизнис, преземете дополнителни мерки за да го заштитите. Овие уреди се вообичаена мета за сајбер криминалците, бидејќи на нив често се чуваат важни датотеки или тие извршуваат важни функции. Потребни се многу стратегии за намалување на инциденти за да се заштитат овие уреди. На пример, важно е да се осигурате дека сите сервери или NAS-уреди редовно се ажурираат. Административните сметки треба да бидат заштитени со сигурна лозинка или мулти-фактор автентикација.
- **Намалете го на минимум „надворешниот отпечаток“:** Проверете и обезбедете ги сите услуги изложени на интернет на вашата мрежа. Ова може да вклучува далечинска работна површина, споделувања на датотеки, веб-пошта и услуги за далечинска администрација.
- **Префрлете се на облак услуги:** Размислете за користење онлајн или облак услуги кои нудат вградена безбедност, наместо самите да управувате со вашата безбедност. На пример, користете онлајн услуги за работи како што се имејли или поставување на веб-страници наместо самите да ги извршувате и обезбедувате овие услуги.
- **Подобрете ја безбедноста на вашиот рутер:** Следете ги нашите упатства за начини за заштита на вашиот рутер, вклучително ажурирање на стандардните лозинки, вклучување на посебен „Гостин“ Wi-Fi за клиенти или посетители и користење на најсигурни протоколи за шифрирање. Пребарајте „router“ на **cyber.gov.au** за повеќе информации.
- **Разберете го вашиот сајбер синџир на снабдување:** Модерните бизниси честопати им даваат на други бизниси да извршуваат повеќе од нивните услуги. На пример, користење на „Управуван испорачувач на услуги“ (Managed Service Provider) за одржување на вашиот ИТ систем. Безбедносните проблеми со овие услуги или доставувачите на услуги може да имаат значително влијание врз вашиот бизнис. За детални совети за управување со ризик во врска со сајбер синџирот на снабдување, прочитајте ги нашите Упатства за сајбер синџири на снабдување на **cyber.gov.au.**

Разговарајте со ИТ професионалец за начини за заштита на вашата мрежа.

Зајакнете ја безбедноста на вашата веб-страница

Веб-страниците се главна мета на сајбер напади.

Заштитете ја вашата веб-страница од „киднапирање“ следејќи неколку основни мерки за безбедност:

- заштитете го најавувањето на вашата веб-страница со мулти-фактор автентикација или сигурна лозинка
- редовно ажурирајте ги системите и дополнителните компоненти за управување со содржината на вашата веб-страница
- редовно правете резервна копија на вашата веб-страница за да можете да ја обновите по сајбер напад.

ACSC има дополнителни материјали за сопствениците на веб-страници. Побарајте ги овие материјали на **cyber.gov.au:**

- Брзи постигнувања за вашата веб-страница
- Воведување на Сертификати, TLS, HTTPS и Опортунистички TLS
- Безбедност на системи на имиња на домени за сопственици на домени
- Подготовка и реакција на напади на одбивање на услуга

Прочитајте ги материјалите на ACSC за безбедност на веб-страници.

Ресетирајте ги вашите уреди пред да ги продадете или отстраните

Податоците на вашите стари уреди може да им бидат достапни на туѓи лица.

Ако не ги отстраните вашите уреди безбедно, сајбер криминалците би можеле да пристапат до податоците на нив. Ова може да вклучува пристап до имејли, датотеки и други деловни податоци. Избришете ги сите податоци од вашите деловни уреди пред да ги продадете, разменувате или отстранете. На пример, со ресетирање на фабричките поставки. Ова ќе помогне да се избришат сите податоци и уредот да се врати на неговите оригинални поставки.

За совети во врска со ресетирање на вашите уреди, прочитајте ги нашите упатства на како безбедно да се ослободите од вашиот уред. Пребарајте „dispose“ на **cyber.gov.au.**

Направете фабричко ресетирање пред да ги продадете или отстраните деловните уреди.

Чувајте ги вашите уреди заклучени и физички безбедни

Со ограничување на пристапот до вашите деловни уреди ќе се намалат можностите за злонамерни активности.

Ограничувањето на физичкиот пристап до вашите деловни уреди е лесен начин да се спречи кражба на податоци или друга злонамерна активност. Деловните уреди не треба да се чуваат на места каде што може да им пристапат неовластени вработени лица или членови на јавноста.

Користете безбедносни контроли за дополнително да ги заштитите вашите деловни уреди. Во најмала рака, тие треба да бидат заклучени со лозинка во форма на фраза, ПИН или биометриска автентикација. Погрижете се овие уреди да бидат поставени на автоматско заклучување по краток период на неактивност.

✓ **Конфигурирајте ги уредите автоматски да се заклучуваат по краток период на неактивност.**

Заштитете ги вашите деловни податоци

Податоците што ги има вашиот бизнис се атрактивна мета за сајбер криминалците.

Прекршувањето на безбедноста на податоци е во пораст - не дозволувајте вашиот бизнис да стане жртва. Важно е да разберете какви податоци има вашиот бизнис и на кои локации. Откако ќе се запознаете со тоа, користете ги препораките во овој водич за да помогнете вашите податоци да бидат заштитени од сајбер криминалци. Некои мали бизниси може да имаат и дополнителни обврски според законот.

- **Консолидирајте ги вашите деловни податоци.** Можеби имате податоци зачувани на многу уреди или во многу служби. Кога податоците се децентрализирани, се зголемува бројот на системи што треба да ги чувате безбедни и да правите резервни копии од податоците што ги содржат. Повеќе системи, исто така, можат да создадат повеќе можности за напад од сајбер криминалец. Секогаш кога е можно, чувајте ги вашите деловни податоци на централна локација што е безбедна и на која редовно се прават резервни копии. Централизирањето на вашите податоци може да создаде поголемо прекршување на безбедноста ако вашите системи се компромитирани, затоа проверете дали оваа централна локација е соодветно заштитена со безбедни поставки и ограничен пристап. Разговарајте со професионалец за ИТ или сајбер безбедност за совети.
- **Познавајте ги вашите обврски за заштита на податоците.** Некои мали бизниси може да имаат законски обврски за тоа како да ракуваат со личните податоци што ги собираат. За да дознаете повеќе, прочитајте го водич за мали бизниси на Канцеларијата на австралискиот началник за информации (Office of the Australian Information Commissioner), достапен на **oaic.gov.au.** Консултирајте се со правно стручно лице ако не сте сигурни.

✓ **Разберете ги податоците што ги има вашиот бизнис и вашите обврски да ги заштитите.**

Подгответе го вашиот персонал

Подучете ги вработените

Вработените со добра пракса во областа на сајбер безбедноста се вашата прва одбрамбена линија против сајбер напади.

Вашите вработени треба да бидат запознаени со сајбер безбедноста, вклучително со следните теми:

- вообичаените закани за сајбер безбедноста, како што се компромитирање на деловен имејл и уценувачки програми
- заштитните мерки вклучувајќи сигурни лозинки или лозинки во форма на фрази, MFA и ажурирање на софтвер
- како да забележат измами и напади преку лажно претставување
- правилата специфични за бизнис (на пример, процедури за пријавување сомнителни имејли или за проверка на валидноста на фактури пред плаќање)

што да прават во итен случај.

На веб-страницата на ACSC има материјали за повеќето од овие теми на cyber.gov.au/learn. Можете да размислите за други начини за подучување на вашите вработени, на пример преку формален курс или интерна обука. Што и да одлучите, запамтете дека обуката за сајбер безбедност не е еднократно барање и треба периодично да се обновува.

✓ **Одлучете како познавањето за сајбер безбедноста ќе се подучува во вашиот бизнис.**

Направете план за итни случаи

План што да се прави во итен случај може да го намали влијанието на сајбер напад врз вашиот бизнис.

Кога реагирате на инцидент во врска со сајбер безбедност, секоја минута е важна. Да се има план за итни случаи значи дека вашиот персонал може да потроши помалку време за да дознае што да прави и повеќе време да преземе мерки.

Размислете за следните прашања кога подготвувате план за итни случаи

- Кој е процесот за вашиот персонал за пријавување на можни инциденти во врска со сајбер безбедноста?
- На кого треба да му се обратите за помош? На пример, ИТ професионалец и вашата банка.
- Како ќе ги известите вашиот персонал, заинтересираните странки или клиентите за инцидентот?
- Како ќе управувате со бизнисот како и обично ако било кои важни системи се исклучени?

Погрижете се вашиот персонал да биде запознаен со планот за итни случаи, вклучувајќи ги сите улоги или одговорности што може да ги има. Чувајте печатена копија од планот во случај вашите системи да се исклучени кога тој ќе ви треба.

✓ **Подгответе план за итни случаи за инциденти во врска со сајбер безбедноста.**

Бидете информирани

Станете партнер на ACSC за да ги добивате најновите информации од нив.

Бидете информирани за најновите сајбер закани и слабости со тоа што ќе станете партнер на ACSC. Оваа служба ќе ви испраќа месечни билтени и предупредувања кога ќе се идентификува нова сајбер закана.

Сајбер безбедноста е област кое брзо се развива. Сајбер криминалците активно ги искористуваат пропустите за неколку минути по нивното откривање. Информирањето за сајбер безбедноста ќе му помогне на вашиот бизнис да ги разбере заканите со кои веројатно ќе се соочи и како да се заштити од нив.

✓ **Пријавете го вашиот бизнис во Програмата за партнерство со ACSC (ACSC Partnership Program).**

Одрекување од одговорност
Материјалот во овој водич е од општ карактер и не треба да се смета како правен совет или материјал на кој можете да се потпирате за помош во било кои одредени околности или итни ситуации. За сите важни работи треба да побарате совети од соодветно независно професионално лице за вашите сопствени околности.

Комонвелтот не прифаќа никаква одговорност или обврска за каква било штета, загуба или трошоци кои произлегуваат поради доверба во информациите во овој водич.

За повеќе информации или да пријавите инцидент, контактирајте нè на:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Овој број е достапен за користење само во Австралија.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre