

# BEZPEČNÝ

# PRODEJ ZISK

# BEZPEČNÝ

Doporučení pro internetové obchody

## 1 PŘIPRAVTE SVŮJ OBCHOD



### KDE BYCH MĚL ZAČÍT?

Budete potřebovat vlastní internetový obchod. Můžete si ho vytvořit sami nebo využít již existující online tržiště. Ať už si vyberete cokoli, nezapomeňte si nechat zaregistrovat jméno a logo své společnosti.

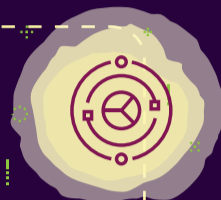


### CO MUSÍM NEJPRVE ZVÁŽIT?

- Vědět, co budu prodávat.
- Vybrat způsob přijímání plateb.
- Vybrat způsob zaslání zákazníkům.
- Ujistit se, že to vše bude probíhat bezpečně.

### JAK SI MÁM VYBRAT PLATFORMU PRO ELEKTRONICKÝ OBCHOD?

Prozkoumejte ta nejdůvěryhodnější tržiště a věnujte pozornost službám a zabezpečení, která poskytují, stejně jako poplatkům, které si účtují.



### CO KDYŽ SI MÍSTO TOHO CHCI VYTVOŘIT VLASTNÍ STRÁNKY?

Můžete si nakonfigurovat modulární systém webového obchodu sami nebo si najmout profesionální společnost, která navrhne a vytvoří Vaše stránky.



### JAK MOHU PRODÁVAT ONLINE?

Abyste mohli prodávat zboží či služby online, budete potřebovat smlouvu s bankou. Hledejte možnost, která bude vyhovovat Vaším potřebám a rozpočtu.



## 2 NASTAVTE SI ZABEZPEČENÍ

### ZÁKLADY KYBER-OCHRANY



Proberte možnosti s bankou a poskytovatelem webových stránek: aktualizujte software, užívejte silná hesla a nainstalujte firewall a antivir. Pokud můžete, využijte pro účely zabezpečení Vašich stránek poskytovatele profesionálních IT služeb.



### POZOR NA VAROVNÁ ZNAMENÍ

Existují nástroje ke kontrole aktivit Vašich zákazníků, které Vám pomohou odhalit, zda jsou skuteční. Sledujte aktuální podvodné trendy ve své zeměpisné oblasti.

### OCHRANA PROTI PODVODŮM



Poznejte své zákazníky za účelem:

- umožnění platby na fakturu nebo požadování platby předem;
- určení způsobu doručení zboží.

Pokud přijímáte platební karty, může Vám poskytovatel poradit nejlepší možnou ochranu proti podvodu.



### OCHRANA DAT

Ujistěte se, že Vaše společnost postupuje v souladu s pravidly GDPR. Vyžádejte si souhlas uživatelů se zpracováním dat. Buďte transparentní v tom, jaká data sbíráte a jak s nimi nakládáte.

### INFORMOVANOST O KYBERNETICKÉ BEZPEČNOSTI



Pokud máte zaměstnance, ujistěte se, že mají povědomí o kybernetické bezpečnosti.

Dbejte, aby si osvojili správné bezpečnostní návyky k ochraně dat společnosti i zákazníků.



### ZÁLOŽNÍ PLÁN

Ujistěte se, že máte plán pro řešení mimořádných událostí. Pravidelně zálohujte své stránky a data na bezpečný server nebo užívejte službu, odkud můžete data obnovit (např. při napadení ransomware).

## 3 PRODÁVAJTE A NECHÁVEJTE SI PLATIT BEZPEČNĚ

### JAK SI MOHU U ZÁKAZNÍKŮ OVĚŘIT...

#### ...PLATBU?

Kontaktujte banku ohledně služby 3D Secure a ujistěte se, že máte nejnovější dostupnou verzi.



#### ...TOTOŽNOST?

Vaše banka Vám poskytne informace o nástrojích a možnostech sloužících k ověření totožnosti Vašich zákazníků.



### JAK MOHOU MOJI ZÁKAZNÍCI PLATIT?

Dostupné způsoby plateb mohou být specifické pro zemi, kde podnikáte. Zjistěte si různé možnosti ohledně: platebních karet, bankovních převodů, objednávek na fakturu, atd.



### JAK MOHU ZAJISTIT BEZPEČNÉ DODÁNÍ SVÉHO ZBOŽÍ?

Úzce spolupracujte se svým dopravcem.

Umožněte změnu místa dodání jen ověřeným zákazníkům a určete, kdy může být dodávka přesměrována a kdy ne.

Zaveďte ověření doručení zboží a potvrzení převzetí zásilky podpisem.

## 4 V PŘÍPADĚ POTŘEBY VYHLEDEJTE POMOC



Obráťte se na společnosti specializující se na pojištění a zmírňování rizik.



Pro další informace navštivte [www.europol.europa.eu/ecomerce](http://www.europol.europa.eu/ecomerce)



Pokud se setkáte s nelegálními aktivitami, kontaktujte policii.