

Subject: **PHISHING**

---

From: **MARTIN ŠEBELA**

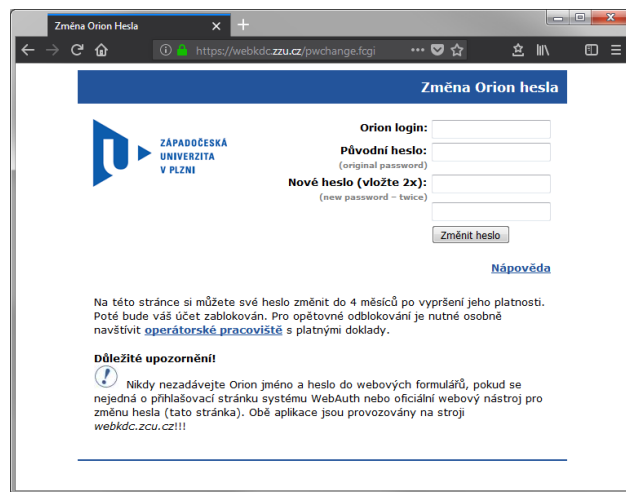
To: **SECFEST ZČU**

Date: **2 Dec 2019**

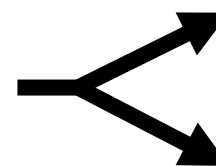
# Phishingator



- Systém pro rozesílání cvičných phishingových zpráv
- V minulosti na ZČU **cvičný phishing** od FLAB CESNET
- Prvotní myšlenka „o phishingu“ po semestrální práci:



*uživatel  
(podvodná stránka pro změnu hesla)*



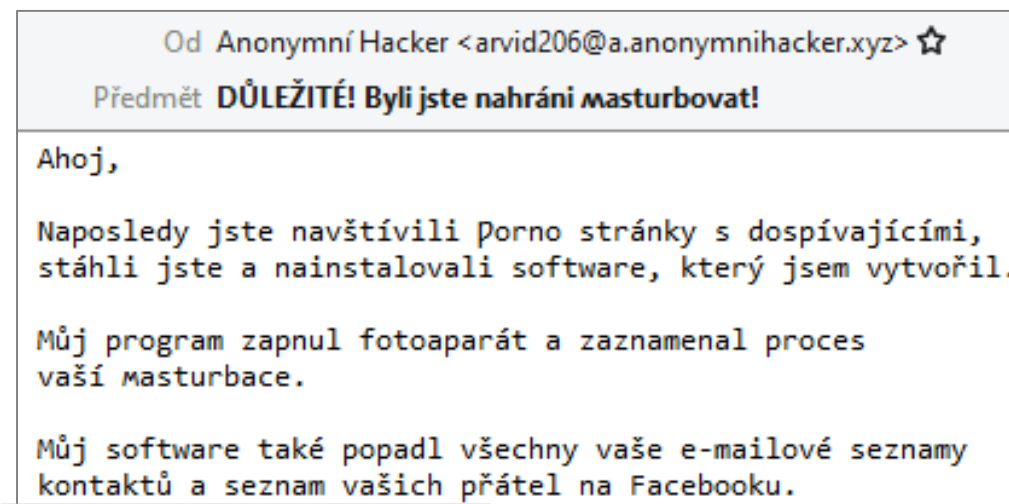
*pravý server*

*útočnickův server*

*uživatelem  
zadané  
údaje*



- **Phishing** = podvodné jednání, pomocí něhož se útočník snaží získat z uživatele důvěrné informace a zneužít je
- Cílem je **poškodit uživatele**
  - Získat **hesla**
  - Získat přístup k **platební kartě**
  - Zneužít **identitu** uživatele
- **Sociální inženýrství**

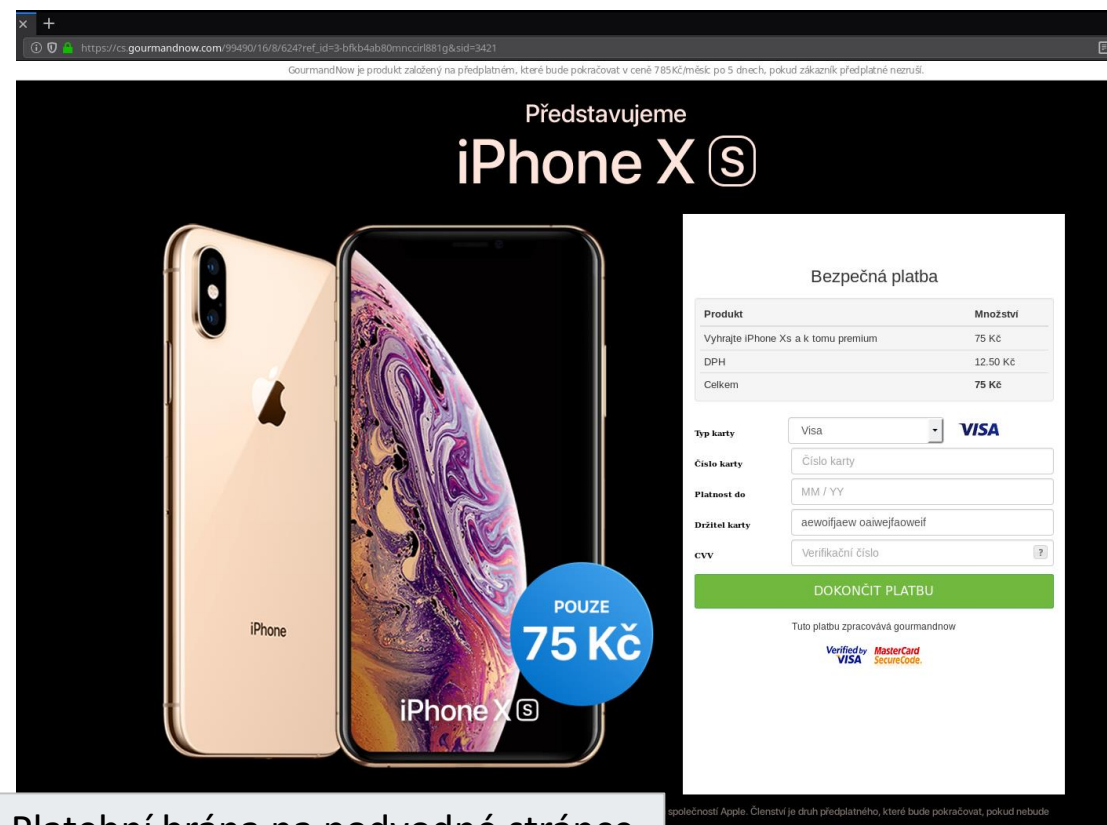


Typický příklad phishingu

# Phishing



- Formou **podvodných e-mailů**, ale i **SMS** a příspěvky na sociálních sítích
- Svázáno s **podvodnými stránkami**
- **Uživatelé** o phishingu často **neví** nebo si jeho **riziko nepřipouští**



Platební brána na podvodné stránce

# Jak může phishing vypadat?



Od Stravovací viceprezident SKM <vice@zcu.cz> ☆

Předmět **Obědové stipendium pro studenti**

Komu msebela@students.zcu.cz ★

Datum Tue, 16 Apr 2019 19:00:02 +0200

Vážený strávníku msebela,  
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným objedům.

Přihlásit se zde: <https://zcu.webkdc.cz/?ha041d1>

Časový limit pro přihlášení je 16. 4. 2019

Bc. et Bc. Jan Hladový  
Stravovací viceprezident  
[vice@skam.zcu.cz](mailto:vice@skam.zcu.cz)  
+555 123 646 888  
SKM, ZČU ve v Plzni

# Jak phishing rozpoznat?



PODEZŘELÁ FUNKCE

Od **Stravovací viceprezident SKM <vice@zcu.cz>** ☆  
Předmět **Obědové stipendium pro studenti**  
Komu msebela@students.zcu.cz ★  
Datum Tue, 16 Apr 2019 19:00:02 +0200

PRAVOPISNÉ CHYBY

Vážený strávníku msebela,  
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným **objedům.**

Přihlásit se zde: <https://zcu.webkdc.cz/?ha041dl>

Časový limit pro **přihlášení** je 16. 4. 2019

PŘEKLEP

Bc. et Bc. Jan Hladový  
Stravovací viceprezident  
[vice@skam.zcu.cz](mailto:vice@skam.zcu.cz)  
+555 123 646 888  
SKM, ZČU ve v Plzni

# Jak phishing rozpoznat?



Od **Stravovací viceprezident SKM <vice@zcu.cz>** ☆  
Předmět **Obědové stipendium pro studenti**  
Komu msebela@students.zcu.cz ★  
Datum Tue, 16 Apr 2019 19:00:02 +0200

Vážený strávníku msebela,  
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným **objedům.**

Přihlásit se zde: <https://zcu.webkdc.cz/?ha041dl>

Časový limit pro **přihlášení** je **16. 4. 2019**

Bc. et Bc. Jan Hladový  
Stravovací viceprezident  
[vice@skam.zcu.cz](mailto:vice@skam.zcu.cz)

**+555 123 646 888**  
SKM, ZCU ve v Plzni

**ČASOVÝ NÁTĹAK**

**PODEZŘELÝ KONTAKT**

# Jak phishing rozpoznat?



Od Stravovací viceprezident SKM <vice@zcu.cz> ☆  
Předmět **Obědové stipendium pro studenti**  
Komu msebela@students.zcu.cz ★  
Datum Tue, 16 Apr 2019 19:00:02 +0200

**PHISHING**

Vážený strávníku msebela,  
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným objedům.

Přihlásit se zde: <https://zcu.webkdc.cz/?ha041d1>

Časový limit pro přihlášení je 16. 4. 2019

Bc. et Bc. Jan Hladový  
Stravovací viceprezident  
vice@skam.zcu.cz  
+555 123 646 888  
SKM, ZCU ve v Plzni

**odkaz na podvodnou stránku vedoucí mimo ZCU . CZ**



# Podvodná stránka



Od Stravovací viceprezident SKM <vice@zcu.cz>  
Předmět **Obědové stipendium pro studenti**  
Komu já <msebela@students.zcu.cz>

Vážený strávnicku msebela,  
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným objedům.

Přihlásit se zde: <http://zcu.webkdc.cz/?ba041dl>

Časový limit pro přihlašování je 16. 4. 2019


Bc. et Bc. Jan Hladový  
Stravovací viceprezident  
[vice@skam.zcu.cz](mailto:vice@skam.zcu.cz)  
+555 123 646 888  
SKM, ZČU ve v Plzni

**PHISHING**

Západočeská univerzita v Plzni - We X +

← → ↻ 🏠 🔒 https://zcu.webkdc.cz/?ba041dl

**Orion WebAuth**

 **ZÁPADOČESKÁ  
UNIVERZITA  
V PLZNI**

**Orion login:**

**Heslo (password):**

[Nápověda](#) | [Nechci se přihlásit](#)

**Kde to jsem? Kam jsem se to zase dostal?**  
Webový server, na který se snažíte přihlásit, byl zařazen do domény jednotného přihlášení (single sign-on, SSO), a vyžaduje ověření vaší identity platným

# Pravá stránka vs podvodná stránka



Browser address bar: <https://webkdc.zcu.cz/login.fcgi?RT=>> (circled in green)

**ZČU**

Orion WebAuth

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Orion login:

Heslo (password):

Přihlásit

[Nápověda](#) | [Nechci se přihlásit](#)

**Kde to jsem? Kam jsem se to zase dostal?**  
Webový server, na který se snažíte přihlásit, byl zařazen do domény jednotného přihlášení (single sign-on, SSO), a vyžaduje ověření vaší identity platným uživatelským jménem a heslem. Stránka, na které se právě nacházíte, je vstupním bodem k webovým serverům ZČU zařazeným pod systém jednotného přihlašování. To znamená, že svoji identitu prokážete skrze tuto stránku prvním serveru, na který chcete přistupovat, a tím jste automaticky přihlášen(a) i k ostatním serverům v doméně.

**Výhody**  
Větší pohodlí pro uživatele (heslo zadávají jen jednou) a technicky vyšší bezpečnost: mezi prohlížečem a webovým serverem se neposílá heslo, ale jen autentizační token. Platnost tokenu je navíc časově omezena.

**Důležitá upozornění!**  
Nikdy nezadávejte Orion jméno a heslo do webových formulářů, pokud se nejedná o přihlašovací stránku systému WebAuth (tato stránka) nebo oficiální webový nástroj pro změnu hesla. Obě aplikace jsou provozovány na stroji [webkdc.zcu.cz](https://webkdc.zcu.cz)!!!

**1**

Browser address bar: <https://zcu.webkdc.cz/?ba0x1dl> (circled in red)

**PHISHING**

Orion WebAuth

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Orion login:

Heslo (password):

Přihlásit

[Nápověda](#) | [Nechci se přihlásit](#)

**Kde to jsem? Kam jsem se to zase dostal?**  
Webový server, na který se snažíte přihlásit, byl zařazen do domény jednotného přihlášení (single sign-on, SSO), a vyžaduje ověření vaší identity platným uživatelským jménem a heslem. Stránka, na které se právě nacházíte, je vstupním bodem k webovým serverům ZČU zařazeným pod systém jednotného přihlašování. To znamená, že svoji identitu prokážete skrze tuto stránku prvním serveru, na který chcete přistupovat, a tím jste automaticky přihlášen(a) i k ostatním serverům v doméně.

**Výhody**  
Větší pohodlí pro uživatele (heslo zadávají jen jednou) a technicky vyšší bezpečnost: mezi prohlížečem a webovým serverem se neposílá heslo, ale jen autentizační token. Platnost tokenu je navíc časově omezena.

**Důležitá upozornění!**  
Nikdy nezadávejte Orion jméno a heslo do webových formulářů, pokud se nejedná o přihlašovací stránku systému WebAuth (tato stránka) nebo oficiální webový nástroj pro změnu hesla. Obě aplikace jsou provozovány na stroji [webkdc.zcu.cz](https://webkdc.zcu.cz)!!!

**2**

# Jak může phishing vypadat?



Od Svatomartinská husa <husa1111@skm.zcu.cz> ☆

Předmět **Svatomartinská husa zdarma**

Komu já <msebela@civ.zcu.cz> ☆

Datum Wed, 6 Nov 2019 07:00:01 +0100

Vážený strávníku, msebela,

v pondělí 11. 11. 2019 nabízí SKM společně se Střední hotelovou školou možnost objednat si porci Svatomartinské husy zdarma. Výdej objednávek bude probíhat po celý výdejní den v salonku v menze Bory. Počet porcí je omezen a je nutné předem si porci zarezervovat a vyčkat na potvrzení. Čím dříve si porci zarezervujete, tím máte větší šanci porci získat. Rezervace budou ukončeny ve čtvrtek 7. 11. 2019 ve 23:59.

Rezervaci proveďte zde: <https://husa1111.webzcu.cz/?ha0201d1>

Evžen Slepíčka  
Šéfkuchař SKM

# Jak phishing rozpoznat?



Od Svatomartinská husa <husa1111@skm.zcu.cz> ☆  
Předmět Svatomartinská husa zdarma  
Komu já <msebela@civ.zcu.cz> ☆  
Datum Wed, 6 Nov 2019 07:00:01 +0100

**PHISHING**

Vážený strávníku, msebela,

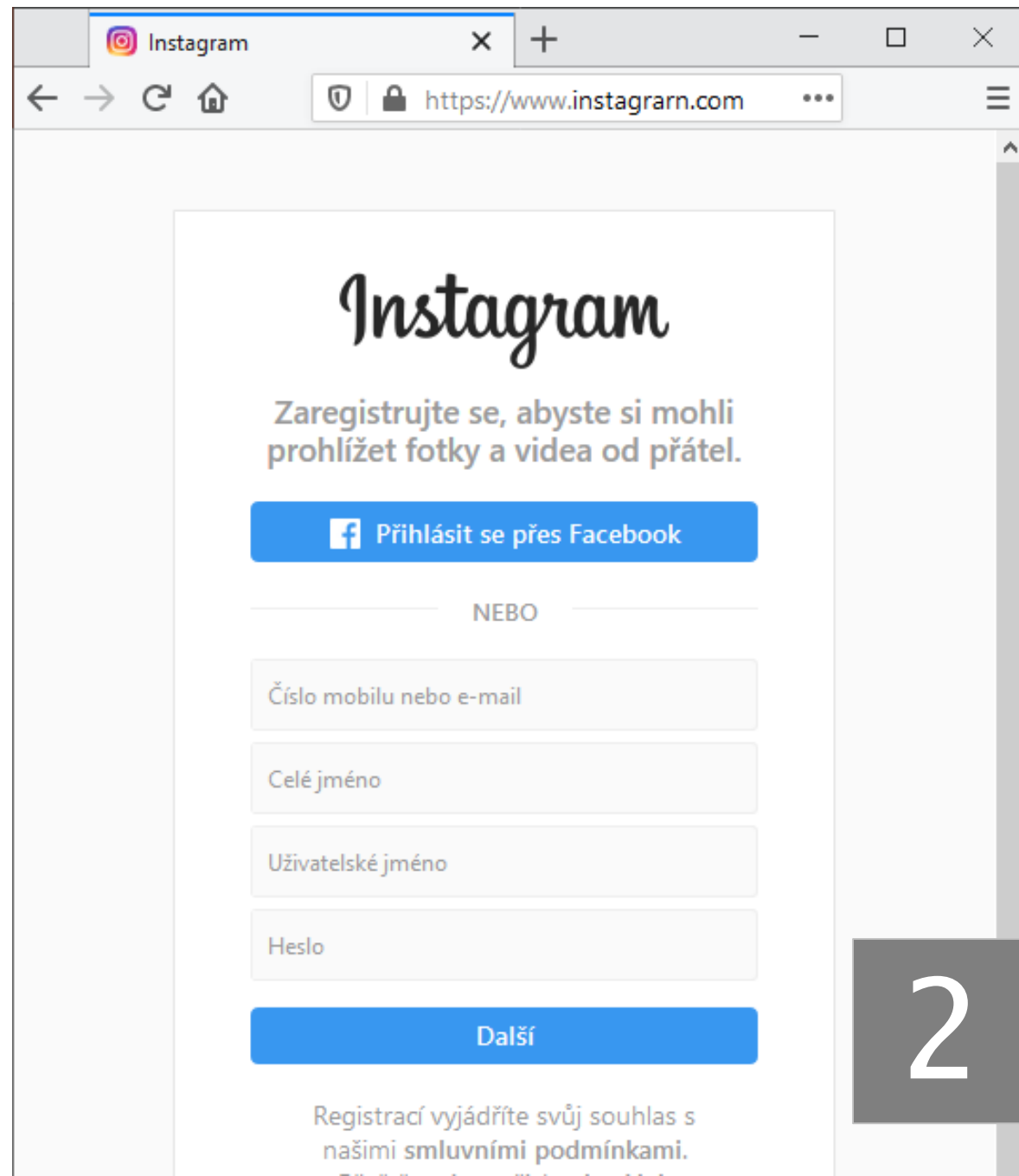
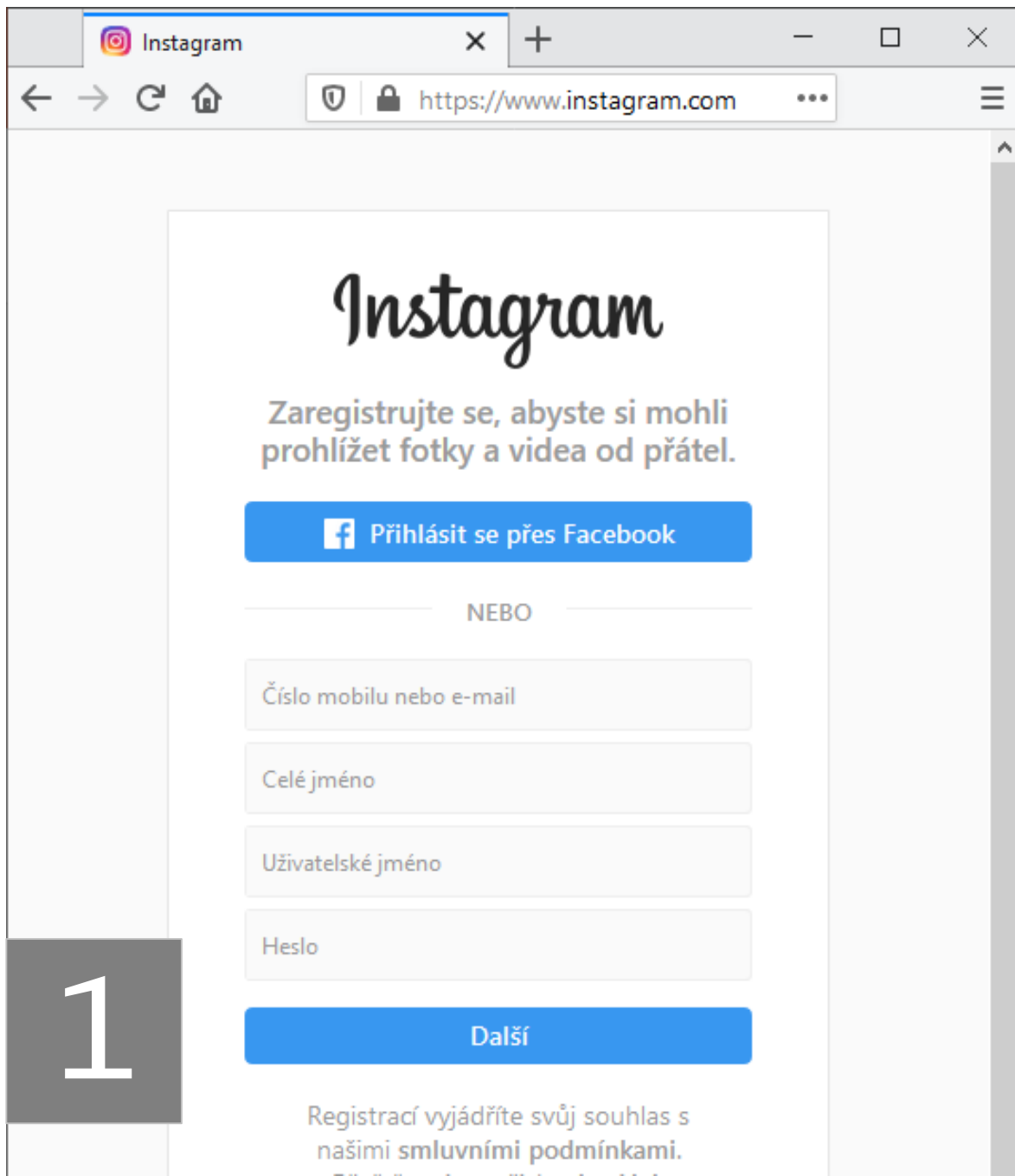
**ČASOVÝ NÁTLAK**

v pondělí 11. 11. 2019 nabízí SKM společně se Střední hotelovou školou možnost objednat si porci Svatomartinské husy zdarma. Výdej objednávek bude probíhat po celý výdejní den v salonku v menze Bory. Počet porcí je omezen a je nutné předem si porci rezervovat a vyčkat na potvrzení. Čím dříve si porci rezervujete, tím máte větší šanci porci získat. Rezervace budou ukončeny ve čtvrtek 7. 11. 2019 ve 23:59.



Rezervaci proveďte zde: <https://husa1111.webzcu.cz/#a0201d1>

Evžen Slepíčka  
Šéfkuchař SKM

**PODVODNÁ STRÁNKA**




Instagram x +

← → ↻ 🏠   https://www.instagram.com

# Instagram

Zaregistrujte se, abyste si mohli prohlížet fotky a videa od přátel.

 Přihlásit se přes Facebook

NEBO

Číslo mobilu nebo e-mail


Celé jméno

Uživatelské jméno



Heslo

**1** Další

Registrací vyjádříte svůj souhlas s našimi smluvními podmínkami.




Instagram x +

← → ↻ 🏠   https://www.instagramarn.com

# Instagram

Zaregistrujte se, abyste si mohli prohlížet fotky a videa od přátel.

 Přihlásit se přes Facebook

NEBO

Číslo mobilu nebo e-mail



Celé jméno

Uživatelské jméno

Heslo

**2** Další

Registrací vyjádříte svůj souhlas s našimi smluvními podmínkami.



# Phishingator



A nechtěl bys jednou za čas poslat cvičný phishing? Abys nezapomněl...

Určitě, znovu se nachytat nechci!



o rozeslání cvičných phishingových zpráv



## Phishingator

Phishing je jako rande – první krok ale udělá vždy útočník a odmítnout můžete jediné Vy.

→ Přihlásit se

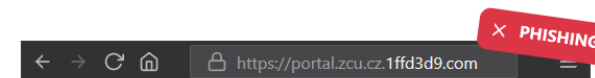
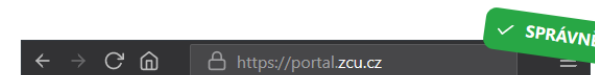
### Co je to ten phishing?

Phishing [fíšing] je **podvodná zpráva**, která uživatele láká na **něco neuvěřitelného**, nebo se mu snaží nějakým způsobem **vyhrožovat** či **napodobovat** jinou známou **instituci/osobu** a jejím jménem uživatele **o něco žádat**.

Útočníci tyto zprávy rozesílají v **obrovském množství**, přičemž jejich **cílem je poškodit uživatele** (a často i instituci, se kterou je e-mail spojen). Z uživatelů se snaží typicky **získat přihlašovací** či jiné **důvěrné údaje** (například **číslo platební karty**).

**Uživatelé** si často bohužel tuto **hrozbu nepřipouští** nebo dokonce o ní **vůbec neví** a **nahrávají tak útočníkům**.

[Více o phishingu »](#)



Pokud **vyplňujete jméno, heslo** nebo cokoliv **důvěrného**, sledujte **adresu webu** až do konce, která může **ukázat na podvod**.

# Přihlášení do Phishingatoru



- **Dobrovolné** odebírání phishingu
- Přihlášení **univerzitním** kontem
  - Studenti i zaměstnanci ZČU
- Možnost kdykoliv změnit účast
- Nastavení **limitu**

## Moje účast v programu


**Ano, chci se dobrovolně přihlásit k odebírání cvičných phishingových zpráv**

To znamená, že několikrát do roka do mé e-mailové schránky dorazí e-mail, který bude obsahovat typické znaky phishingu a sociálního inženýrství. Na rozdíl od toho reálného mi ovšem ten cvičný nic neprovede ani neukradne.

Omezit počet zpráv, které mi budou zaslány (nepovinné)

Zbývající počet cvičných phishingových zpráv, o které mám zájem

Po odeslání každé zprávy dojde ke snížení tohoto čísla. Po dosažení nuly nebude zaslána žádná další zpráva, dokud toto číslo opět nezvýšíte.

 Změnit mé nastavení



# Phishingator

- Cílem **vzdělat uživatele**
- Upozornění na **indicie**
  - V podvodném **e-mailu**
  - Na podvodné **stránce**
- **Notifikace**
- **Osobní statistika**

## Phishingator

### Právě jste absolvovali **cvičný phishing**

Děkujeme, že máte zájem **vzdělávat se** v oblasti **phishingu**. Jakékoliv **změny** včetně nastavení **limitu cvičných e-mailů** můžete provést po **přihlášení** do Phishingatoru (ZČU).

[→\] Více informací...](#)

### Jak bylo možné **phishing** rozpoznat **z e-mailu**

Od: Svatomartinská husa <husa1111@skm.zcu.cz>  
Předmět: Svatomartinská husa zdarma  
Komu: msebela@civ.zcu.cz  
Datum: 6. 11. 2019 7:00

Vážený strážníku, msebela,

v pondělí 11. 11. 2019 nabízí SKM společně se Střední hotelovou školou možnost objednat si porci Svatomartinské husy **zdarma**. Výdej objednávek bude probíhat po celý výdejní den v salonku v menze Bory. Počet porcí je omezen a je nutné předem si porci zarezervovat a vyčkat na potvrzení. **Čím dříve** si porci zarezervujete, tím máte větší šanci porci získat. Rezervace budou ukončeny ve čtvrtek 7. 11. 2019 ve 23:59.

Rezervaci proveďte zde: <https://husa1111.webzcu.cz>

**Evžen Slepíčka**  
Šéfkuchař SKM

#### **1. indicie** Časový nátlak

Útočníci často využívají časový nátlak, aby obětem nedali prostor nad přemýšlením.

[^ Zruš označení](#)

#### **3. indicie** URL vede mimo doménu ZČU

Správná adresa v doméně ZČU je <cokoli>.zcu.cz/<cokoli> - oddělovač je tečka

[^ Zruš označení](#)

#### **4. indicie** Není zaměstnanec ani SKM ani ZČU

Možno ověřit na webu [www.zcu.cz](http://www.zcu.cz) (sekce Zaměstnanci v menu).

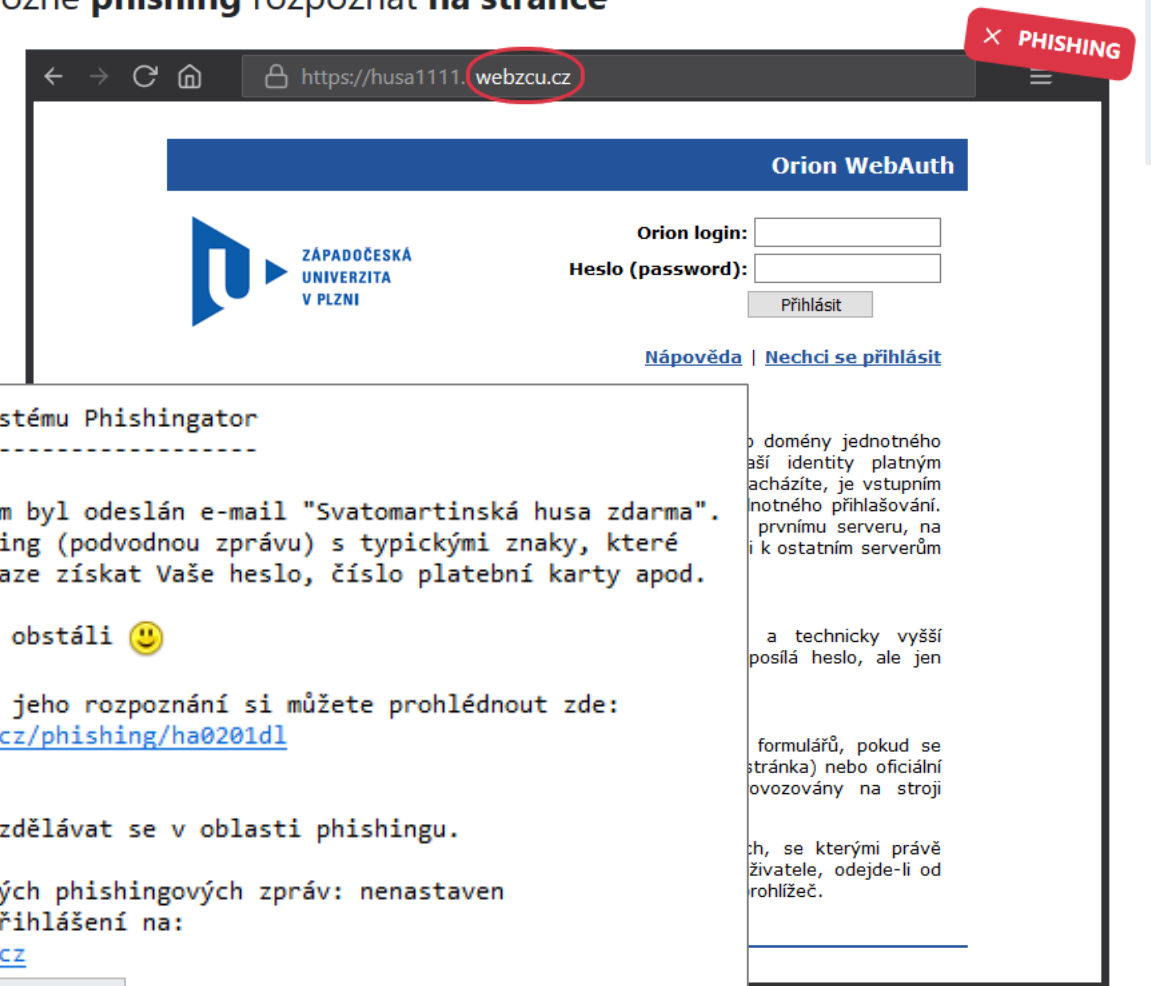
[^ Zruš označení](#)

#### **2. indicie** Psychologický nátlak

# Phishingator

Jak bylo možné **phishing** rozpoznat **na stránce**

- Cílem **vzdělat uživatele**
- Upozornění na **indicie**
  - V podvodném **e-mailu**
  - Na podvodné **stránce**
- **Notifikace**
- **Osobní statistika**



Notifikace z Phishingatoru

## 1. indicie Špatná adresa stránky

Snaha o napodobení pravé URL adresy – je třeba sledovat adresu webu až do jejího konce. Správná adresa v doméně ZČU je <cokoli>.zcu.cz/<cokoli> - oddělovač je tečka

^ Zruš označení

Indicie k podvodné stránce

- Úvodní stránka
- Kampaně
- Podvodné e-maily
- Podvodné stránky
- Uživatelé
- Skupiny

## Kampaně

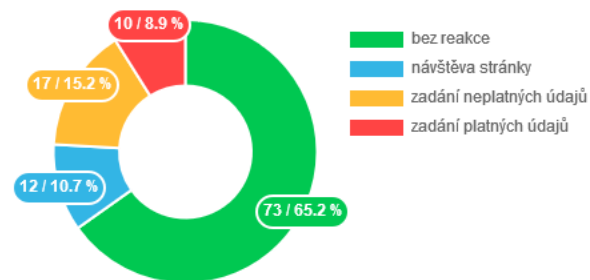
[Seznam kampaní](#)

Tato sekce slouží k vytváření nových a správě dosud vytvořených kampaní. Každá z kampaní je svázána se zvoleným [podvodným e-mailem](#) a [podvodnou webovou stránkou](#), na kterou se příjemce e-mailu dostane právě z obsahu tohoto e-mailu (pokud bude následovat odkazy v něm uvedené). Podrobnější informace jsou k dispozici v dostupné [nápovědě](#).

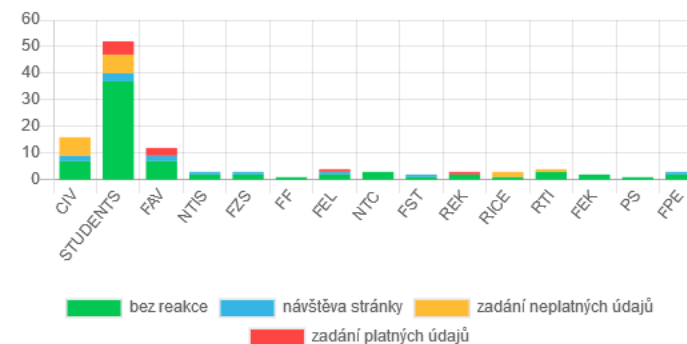
## Základní informace

Název	Přidáno	Přidal	Podvodný e-mail	Podvodná stránka	URL podvodné stránky	Odesláno e-mailů	Spuštění rozesílání	Aktivní od	Aktivní do
Svatomartinská husa	5. 11. 2019	cepakj	Svatomartinská husa	<a href="#">Náhled</a> Stránka určená k e-mailu o svatomartinské huse (WebAuth ZČU, přihlášení (věrná kopie))	<a href="#">https</a> ://husa1111.webzcu.cz	<a href="#">Náhled</a> 112/112	každý den od 7:00	6. 11. 2019	7. 11. 2019

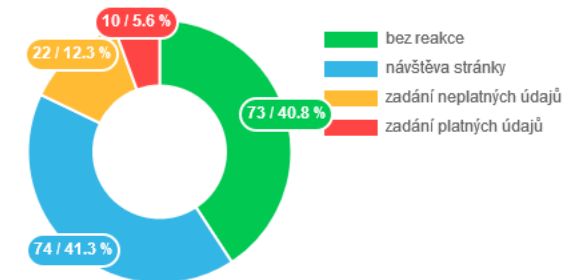
### Konečné akce uživatelů v kampani


[Tabulka konečných akcí](#)

### Konečné akce v kampani dle skupiny



### Provedené akce v kampani


[Tabulka všech provedených akcí](#)

<https://phishingator.zcu.cz>



phishingator



Vše

Obrázky

Mapy

Video

Nákupy

Více

Nastavení

Nástroje

Přibližný počet výsledků: 65 (0,31 s)

**Phishingator · Systém pro rozesílání cvičných phishingových ...**

<https://phishingator.zcu.cz> ▾

**Phishingator** | Systém pro rozesílání cvičných phishingových zpráv.

# Shrnutí

- Pozor na typická lákadla – „**zdarma**“, **výhra**, **časový nátlak**, **vyhrožování**
- Kontrola **adresy** webu
- Podvodné stránky mohou vypadat vizuálně **naprosto stejně** jako ty pravé
- **Phishingator** – phishing, který nebolí

Podvodná stránka



11. listopadu 2018

Děkujeme za vyplnění našeho dotazníku! Máme následující nabídky, kterých se můžete zúčastnit: **Neděle, 11. listopadu 2018**. Vyberte si prosím z kterékoliv níže uvedené nabídky (1) pouze dnes:



**Apple iPhone XS**

Zbývající množství: **1**

Běžná cena: **40-490 Kč**

Pouze dnes: **25 Kč**

[Klikněte zde →](#)

Unlike Komentář Sdílet

143

**Radana Konrádová** Díky!!!  
Unlike · Odpovědět · Právě teď

**Borek Prokop** Jsem tak rád, že jsem vyhrál! Zadal jsem svůj e-mail a teď už jen čekám, než mi iPhone dorazí :)  
Unlike · Odpovědět · Právě teď

**Zoe Hošková** #ráda  
To se mi líbí · Odpovědět · Právě teď

**Pravoslav Holeček** Zrovna dnes mi dorazil iPhone. Moc děkuji!  
Unlike · Odpovědět · Právě teď

**Růt Uherková** Moje odměna dnes dorazila. Díky za iPhone!!!  
Unlike · Odpovědět · Právě teď

**Jeroným Zapletal** Fantastické! Nikdy předtím jsem nic nevyhrál, ale doufám, že budu mít štěstí!  
Unlike · Odpovědět · Právě teď

**Lubor Rušil** Ten kvíz byl až moc lehký, tak doufám, že iPhone opravdu dostanu!  
Unlike · Odpovědět · Právě teď

**Arnošt Suchánek** Je tohle vtip?  
Unlike · Odpovědět · Právě teď



**Martin Šebela**  
msebela@civ.zcu.cz