**Externí**

**Označení od neznámého na Facebooku či jiné sociální síti**

Sleva na oblečení / drogerii / zahradní vybavení

Výzva k úhradě / faktura po splatnosti

**Zásilka k vyzvednutí / doplatek - Česká pošta, DHL, PPL...**

Hacknutí / zašifrování PC - vydírání

**Interní**

Změňte si heslo, bylo Vám resetováno heslo...

**Dochází místo v e-mailové schránce**

**Přihlášení z cizího zařízení/lokace**

Nové benefity pro zaměstnance

Pozastavení účtu k interní službě

Nastavení výjimek v antiSPAMových a antivirových enginech je stěžejní pro nezkreslené výsledky phishingových testů. V tomto článku si ukážeme, jak jednotlivé výjimky nastavit.

Výjimky v antiSPAMu

Výjimky v antiSPAMu by měly být tyto:

Doména mailserveru: [mail.privacyfreak.net](https://mail.privacyfreak.net/)

IP mailserveru je: 37.205.13.44

A na odesílatele:

[notification@maildelivery.cz](mailto:notification@maildelivery.cz)

[upozorneni@ceskapocta.cz](mailto:upozorneni@ceskapocta.cz)

[info@nase-benefity.cz](mailto:info@nase-benefity.cz)

[facebook@mailingserver.eu](mailto:facebook@mailingserver.eu)

[notification@mlcrosoft365.cz](mailto:notification@mlcrosoft365.cz)

+ další dle dohodnutých scénářů

URL:

Pokud má mailserver i antivirový modul, přidejte prosím domény i do něj se znakem „\*“ před i za doménou. ( \*ceskapocta.cz\*, \*doména\_dle\_scénáře\*,...)

V momentě kdy nastavíte výjimky na Exchange/mailserveru, přijde e-mail normálně do doručené pošty. Je nezbytně nutné nastavit výjimky a přidat domény na whitelist / do bezpečných odesílatelů.

Nastavení v MS Exchange

V případě phishingové simulace je pravděpodobné, že některé z těchto emailů jsou identifikovány jako spam/phishing a přesunuty do složky Nevyžádaná pošta v aplikaci MS Outlook. Je tedy třeba je přidat na whitelist – seznam povolených domén, kdy takto označené domény obcházejí spamový/phishingový filtr.

Byť většinou je uživatelské rozhraní v angličtině, stejně jako přiložené screenshoty, textový návod uvádíme pro ty co preferují mateřský jazyk v češtině.

V prostředí **Office 365 – Exchange online** je třeba provést přidání pravidla pro příchozí poštu pomocí **Centra pro správu Exchange**. V položce **tok pošty – pravidla** zvolte nové pravidlo s názvem **Vynechat filtrování spamu**….

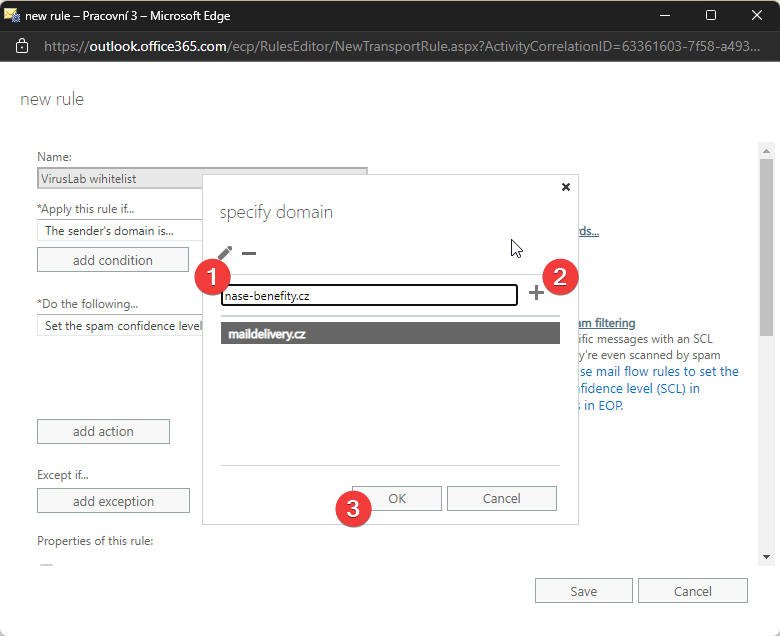
[Obsah obrázku text

Popis byl vytvořen automaticky](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101002550610/original/P5itqy0F-ploiP3s4Fn5DX6sXFG7d3qvyQ.png?1642492036)

[Obsah obrázku text

Popis byl vytvořen automaticky](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101002550549/original/tDtGw1CdtFGTaeNUFGva-LjlH7fY57VH6w.png?1642491928)

Nové pravidlo si nazvěte dle potřeby, například „VirusLab whitelist“ a v sekci podmínek zvolte možnost **Odesílatel – doména je** .

[](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101002550569/original/MHjnxXh7eF4gHP1_OmccaAWCcMh1mlYqHg.png?1642491975)

V seznamu domén, sepište seznam požadovaných domén (viz. výše) do whitelistu a po uložení je hotovo.

Výjimky v antivirových programech

V antiviru (na koncových stanicích) prosím nastavte v modulech HTTP skenování a AntiPhishing modulu tyto adresy – i se znakem \* aby došlo k vyloučení subdomén a dalších částí URL. Toto nastavení provádějte prosím v centrální konzoli, tak aby došlo k propsání výjimek na všechny koncové stanice.

Standardní domény které používáme:

\*nase-benefity.cz\*

\*maildelivery.cz\*

\*mailingserver.eu\*

\*ceskapocta.cz\*

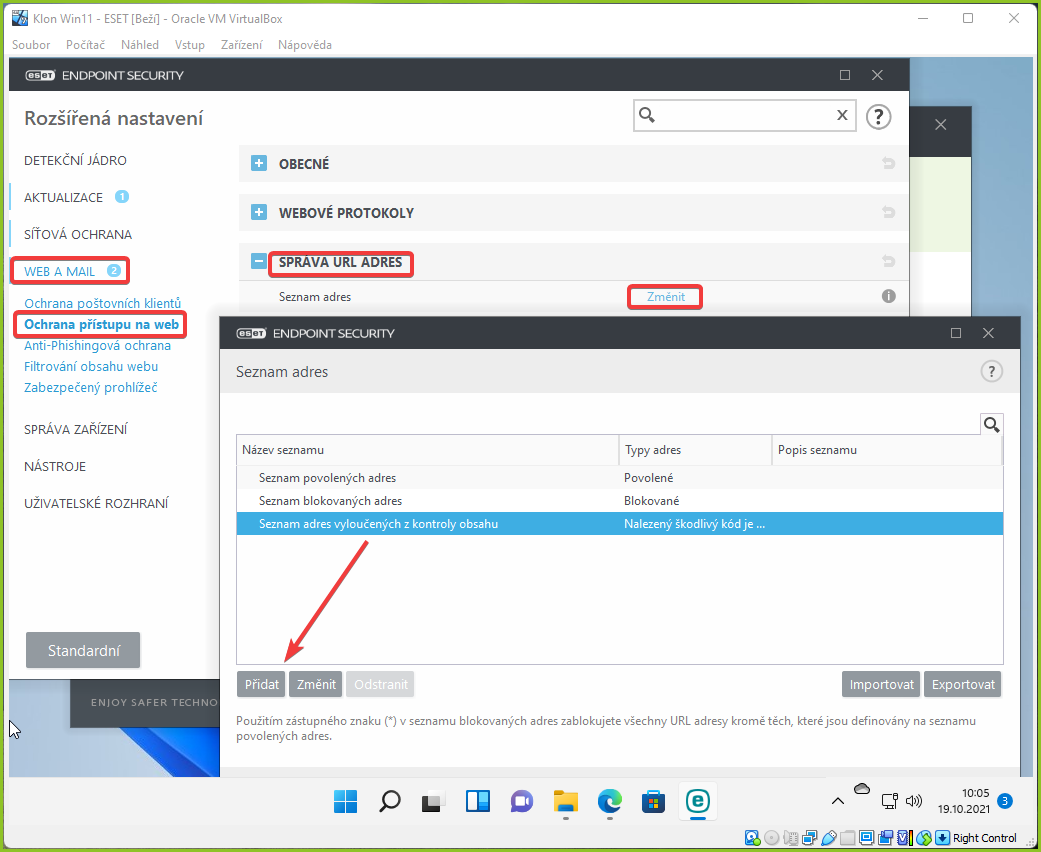
\*mlcrosoft365.cz \*

*Konkrétní domény závisí vždy na dohodnutém scénáři.*

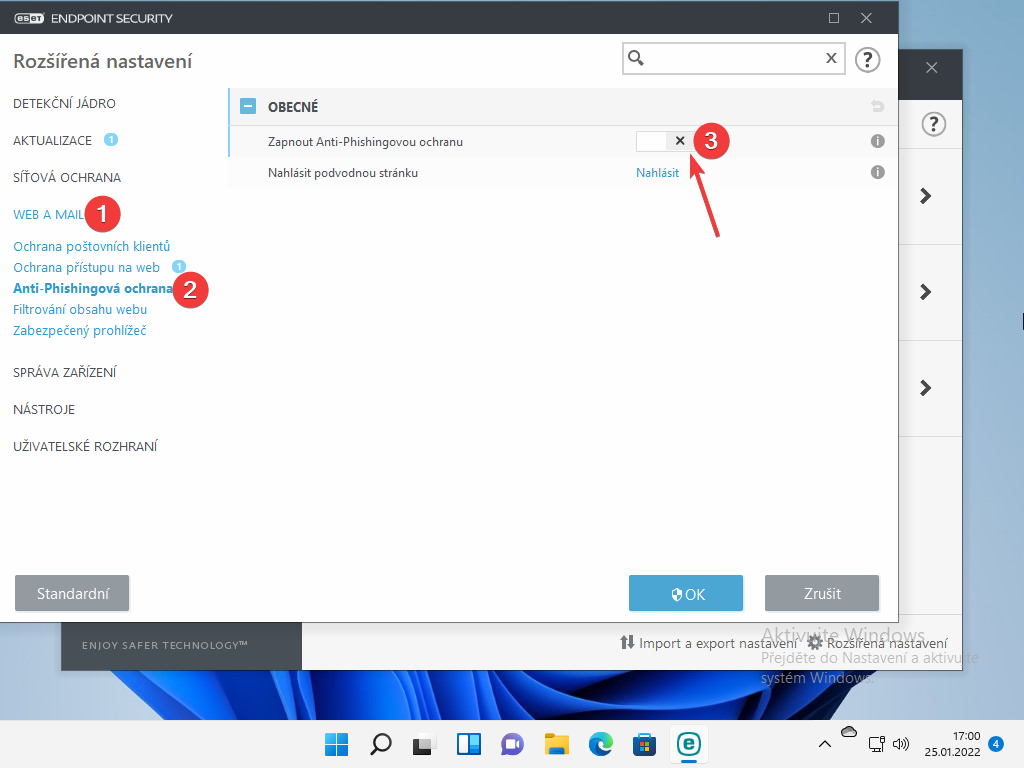
Toto zabrání detekci na koncových stanicích a umožní načtení obsahu e-mailů a přesměrování na stránky v případě ,že by antimalware řešení lokálně rozpoznalo phishing a dalo to vědět ostatním stanicím v síti.

ESET

Výjimku lze přidat v rozšířeném nastavení (Vyvoláte stiskem F5) a pak v sekci **Web a mail – Ochrana přístupu na web – Správa URL adres** klikněte na **Změnit** u **Seznamu adres**. Zde přidejte *\*maildelivery.cz\** (včetně hvězdiček!) do **Seznamu adres vyloučených z kontroly obsahu**.

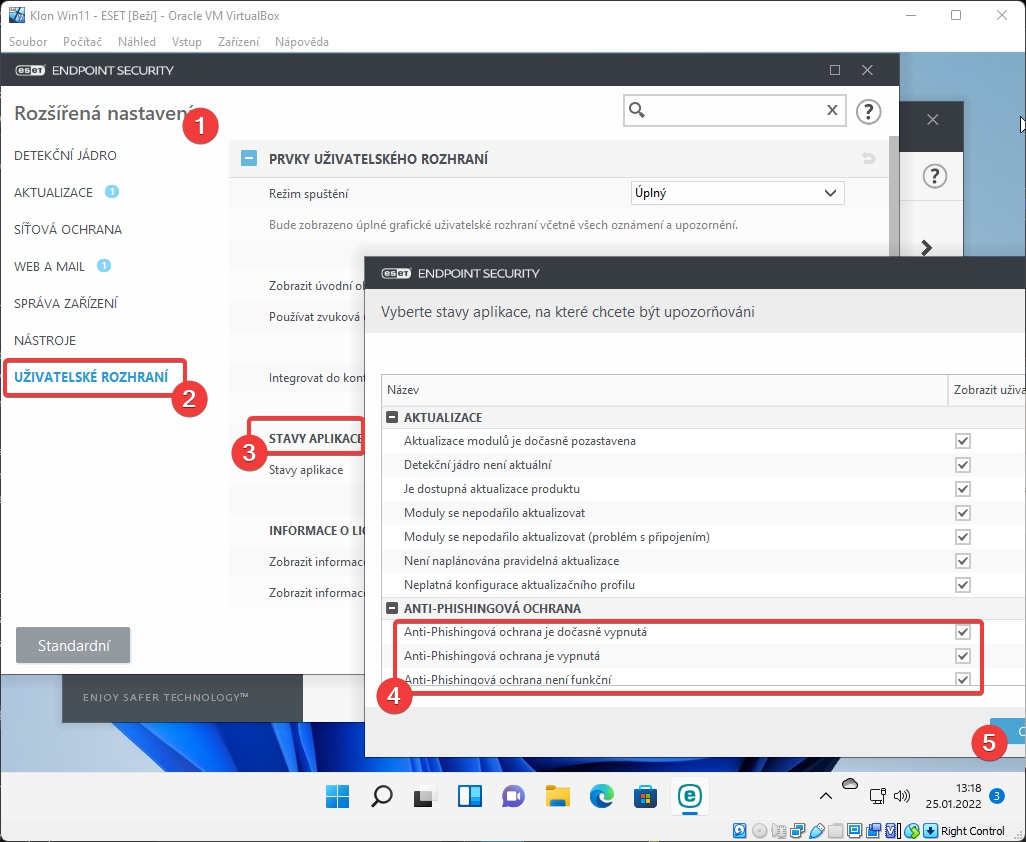
[](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101000181965/original/BdVx8tj8s11_5LBGFNoZQtSVBAhJ1uxG4g.png?1635608286)

Současně vypněte také samostatný **Anti-Phishing** modul který se nachází v sekci **Anti-Phishingová ochrana**.

[](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101003336416/original/tIRzL1mzErmyneghThw8kfWE7L-45BilHg.png?1643374053)

Ukázka je na koncové stanici, nicméně změny provádějte ideálně z konzole**ESET Protect** pomocí [politiky](https://help.eset.com/protect_admin/80/cs-CZ/admin_pol.html), kterou aplikujte na všechny stanice, na které bude phishingový test probíhat.

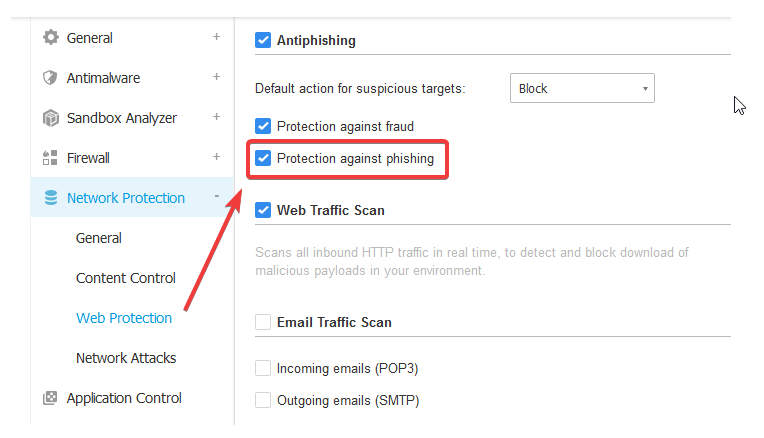
Aby uživatelům ESET nehlásil, že je modul Antiphishing vypnutý (GUI pak svítí červeně), nastavte politikou vypnutí tohoto **Stavu aplikace**.

[](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101003336336/original/RjjR8yAFiwJpOG5ykcVHyoYrWNzEMUAufw.png?1643373960)

Bitdefender

Řešení Bitedefenderu spolupracuje s Exchange, takže výjimky v AntiSPAMu stačí mít nastavené tam. Nicméně je možné je nakonfigurovat i přímo v GravityZone: [Configuration (bitdefender.com)](https://www.bitdefender.com/business/support/en/77209-79937-configuration.html)

Co se týče blokace anti-phishing modulem, tak jeho nastavení je popsáno zde: [Configuration (bitdefender.com)](https://www.bitdefender.com/business/support/en/77209-88324-network-protection-configuration.html" \l "UUID-8a479878-c62b-e5ff-c405-48b75031a1c4)

[](https://s3-eu-central-1.amazonaws.com/euc-cdn.freshdesk.com/data/helpdesk/attachments/production/101002548448/original/UalHrC6jAl9vXpgQxwv2ajOwYKE3ulGD9Q.png?1642488443)

Výjimky ve Firewallu

Pokud filtrujete odchozí komunikaci, povolte prosím port **444**.

Všechny uvedené typy výjimek považujte prosím za dočasné! Po ukončení kampaně je potřeba je deaktivovat či odstranit, aby nedošlo k otevření potenciálního vektoru pro zneužití.