

1. Dvoufaktorové zabezpečení účtů (2FA)

Filip Szkorupa

| | |
|-----------------------------------|--|
| Oblast z RVP Doporučený stupeň | Digitální technologie 2. stupeň ZŠ, nižší ročníky SŠ |
| Naplněvané výstupy RVP | <ul style="list-style-type: none">dokáže usměrnit svoji činnost tak, aby minimalizoval riziko ztráty či zneužití dat; popíše fungování a diskutuje omezení zabezpečovacích řešení |
| Vstupní požadavky na žáky | Žák umí pracovat běžným způsobem na lokální stanici, chytrém zařízení, orientuje se v prostředí internetu a webových služeb. |
| Cíl aktivity | <ul style="list-style-type: none">Žáci pochopí princip dvoufaktorové autentizaceŽáci umí nastavit 2FAŽáci chápou důležitost zabezpečení účtůŽáci rozvíjí slovní zásobu anglického jazyka |
| Rozvíjené kompetence | Kompetence k učení <ul style="list-style-type: none">Získává hlubší přehled o bezpečnosti vlastních účtůExperimentuje s různými možnostmi nastavení zabezpečení účtů a posuzuje jejich vhodnost Kompetence k řešení problémů <ul style="list-style-type: none">Užívá při řešení problémů logické postupyDokáže zvolit efektivní způsob zabezpečení svých účtů Kompetence komunikativní <ul style="list-style-type: none">Vysvětlí princip zabezpečení účtu pomocí 2FADokáže popsat důvody zabezpečení pomocí 2FA |
| Potřebné vybavení | <ul style="list-style-type: none">Zařízení připojené k internetu (PC, Notebook)Smartphone pro dvoufázové ověřováníÚčet Google nebo Apple, účty sociálních sítíAplikace Authenticator |
| Časová dotace | 2-3 vyučovací hodiny |

Příprava na výuku

- Ve své podstatě je důležité to, aby žáci měli přístup ke svým Google účtům.
- Počítače by měly mít nainstalovanou aktuální verzi Google Chrome.
- Každý z žáků by měl disponovat chytrým zařízením (Smartphone s OS Android nebo iOS).
- Pedagog může zadat žákům, aby si doma nainstalovali aplikaci Authenticator, ale není to nutnost, jelikož instalace aplikace je součástí výuky.

Organizace práce

1. Úvod do problematiky

Cílem hodin je seznámit žáky a studenty se sofistikovanými možnostmi zabezpečení jejich účtů, které jsou ve většině případů chráněny jednoduchým heslem. Žáci používají stejné e-maily a hesla pro různé služby, tím však ohrožují svou digitální identitu. E-mail a heslo jsou dnes prakticky vstupní bránou ke všem službám a osobním informacím. Proto je důležité myslet na vyšší úroveň zabezpečení.

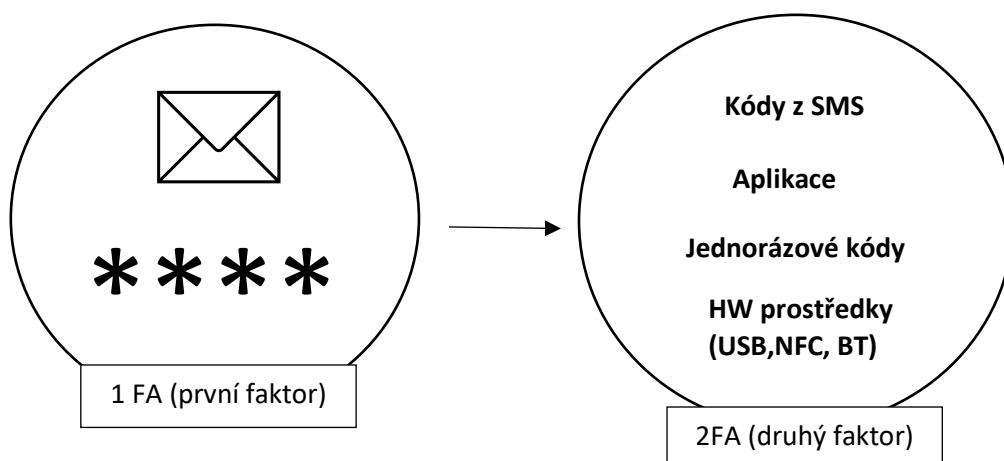
Otázka na žáky: Jaké formy zabezpečení používáte na svých účtech?

2. Princip použití 2FA

V dnešní době využívá většina webových služeb, snad jen až na výjimky, tento typ ochrany. Jedná se o proces, kdy se uživatel přihlašuje ke službám, aplikacím a sociálním sítím pomocí více důkazů o jeho identitě.

Žákům vysvětlíme smysl a princip využití 2FA a obecně MFA (vícefaktorové ověřování) například pomocí stránek:

<https://www.google.com/landing/2step/index.html>. Případně používáme schémata.



Zdůrazníme, že 2FA lze nastavit na různých účtech. Princip je vždy stejný s tím, že každá služba ukrývá nastavení pod jiným názvem (ochrana soukromí, zabezpečení, přihlášení a bezpečnost, nastavení a soukromí).

3. Nastavení různých možností 2FA

Pedagog demonstruje nastavení 2FA na svých účtech. Pro výuku budeme používat Google účty, jelikož většina žáků tímto účtem disponuje. Ovšem rozhodnutí je na samotném pedagogovi, kterou službu využije. Žákům je důležité také říci, že se jedná o kroky, které lépe zabezpečí jejich účty ovšem na úkor komfortu.

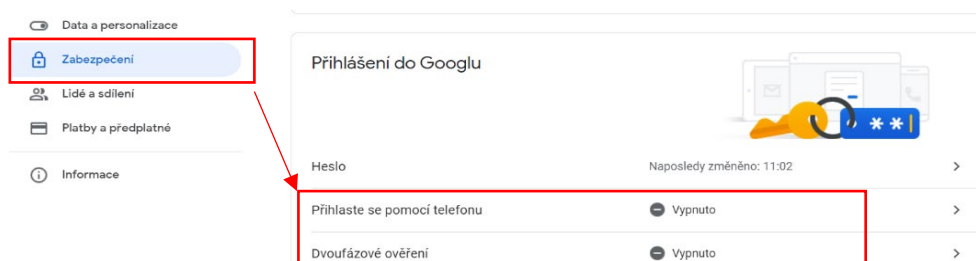
Pokusíme se s žáky nastavit různé možnosti zabezpečení 2FA:

- 1) výzvy od Google,
- 2) jednorázové kódy,
- 3) aplikace Authenticator

Pedagog si, dle náročnosti a šikovnosti žáků, může vybrat jen jednu možnost. Samotná aktivita žáků probíhá na školních počítačích, vhodné je také zařazení BYOD, resp. si to následující činnosti přímo vyžadují.

Postup nastavení 2FA

- 1) Žáci se přihlásí ke svým účtům a zapnou dvoufázové ověření



2) S žáky nastavíme zabezpečení pomocí **výzev (jednorázových kódů)**, které uživatel dostává na telefon (Android, iOS) přihlášený k účtu. Nastavení je velmi intuitivní. Se žáky postupujeme krok za krokem, v případě obtíží individuálně řešíme komplikace například nezobrazení mobilního zařízení, na které má být výzva poslána.

Google Účet → Zabezpečení → Přihlaste se pomocí telefonu Vypnuto
Dvoufázové ověření Vypnuto

← Dvoufázové ověření

Zabezpečte svůj účet pomocí dvoufázového ověření
Při každém přihlášení k účtu Google bude potřeba zadat heslo a ověřovací kód. [Další informace](#)

- Přidejte další úroveň zabezpečení**
Zadejte heslo a jedinečný ověřovací kód, který byl zaslán do vašeho telefonu.
- Chraňte svůj účet před padouchy**
I kdyby někdo zjistil vaše heslo, k účtu se nebude moci přihlásit.

ZAČÍNÁME

Nyní váš telefon nastavíme

Jaké telefonní číslo chcete používat?

🇨🇪 _____

Společnost Google toto číslo použije pouze k zabezpečení účtu. Nepoužívejte číslo Google Voice. Za zprávy a data vám operátor může účtovat poplatky.

Jakým způsobem si přejete získávat kódy?

Textová zpráva Telefonní hovor

Zobrazit další možnosti

Bezpečnostní klíč
Malé fyzické zařízení, které slouží k přihlašování

Výzva od Googlu
Nechte si do telefonu zasílat výzvy od Googlu a přihlašujte se klepnutím na Ano

← Dvoufázové ověření

Používejte telefon jako druhý krok při přihlašování
Po zadání hesla bude do každého telefonu, ve kterém jste přihlášení, bezpečně odeslána výzva od Googlu. Stačí klepnout na oznámení a přihlásit se.

Tato zařízení mohou dostávat výzvy

Huawei P20 lite **Viditelné zařízení**

Zařízení nevidíte? **Pokud zařízení nevidíme**

Zobrazit další možnosti

POKRAČOVAT

Může nastat komplikace – uživatel musí nastavit svůj účet na telefonu

← Dvoufázové ověření

Připravte zařízení pro dvoufázové ověření
V telefonu Android nebo v iPhone se přihlaste k účtu Google.

Na telefonu Android:

- Otevřete aplikaci **Nastavení**.
- Klepněte na **Účty** a poté na **Přidat účet**.
- Vyberte **Google** a přihlaste se.

Na iPhone:

- Z obchodu App Store si stáhněte aplikaci **Google**.
- Přihlaste se pomocí účtu Google.

ZAVŘÍT **ZKUSIT ZNOVU**

POKRAČOVAT

Už to bude! Přidejte záložní možnost
Pokud ztratíte telefon nebo váš druhý krok nebude k dispozici, budete potřebovat záložní možnost, jak se do účtu dostat.

Společnost Google toto číslo použije pouze k zabezpečení účtu. Nepoužívejte číslo Google Voice. Za zprávy a data vám operátor může účtovat poplatky.

Jakým způsobem si přejete získávat kódy?

Textová zpráva Telefonní hovor

POUŽÍT JINOU ZÁLOŽNÍ MOŽNOST

ODESLAT

← Dvoufázové ověření

Zapnout dvoufázové ověření?

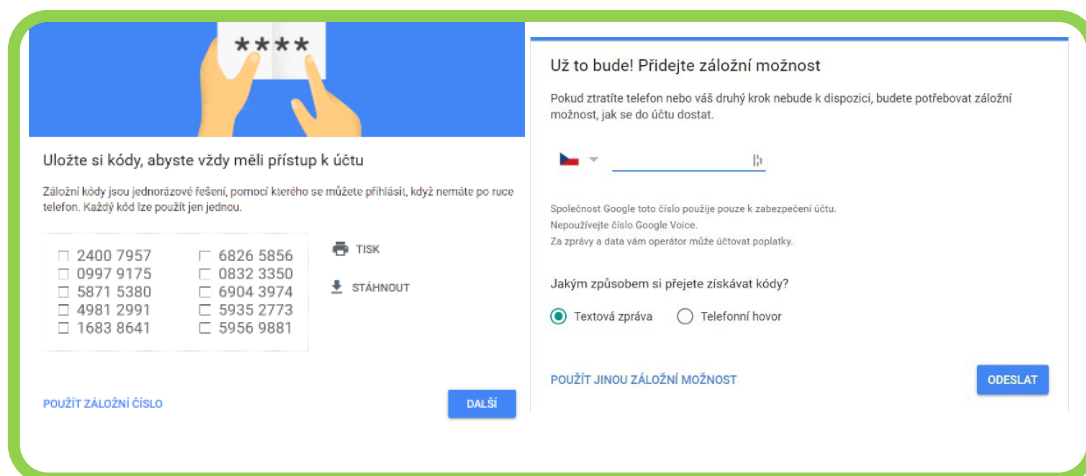
Druhý krok: **Výzva od Googlu (výchozí)**
Záložní možnost: **Hlasová zpráva nebo SMS**

V následujících zařízeních zůstanete přihlášení k účtu **Scrufa@centrum.cz: Huawei P20 lite**.

Z ostatních zařízení můžete být odhlášení. K opětovnému přihlášení bude třeba použít heslo a druhý krok.

ZAPNOUT

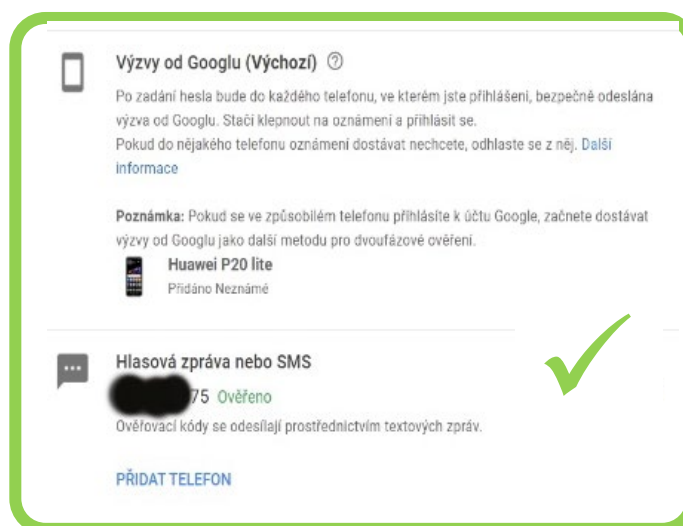
V další části můžeme s žáky nastavit alternativní možnosti přihlášení pomocí jednorázových kódů nebo telefonního hovoru.



The screenshot shows the Google account recovery interface. On the left, there's a section titled "Uložte si kódy, abyste vždy měli přístup k účtu" (Save codes so you always have access to your account). It lists several backup codes in a grid: 2400 7957, 0997 9175, 5871 5380, 4981 2991, 1683 8641, 6826 5856, 0832 3350, 6904 3974, 5935 2773, and 5956 9881. There are also buttons for "TISK" (Print) and "STÁHNOUT" (Download). Below the codes is a "POUŽÍT ZÁLOŽNÍ ČÍSLO" (Use backup code) button and a "DALŠÍ" (Next) button.

On the right, there's a section titled "Už to bude! Přidejte záložní možnost" (That's it! Add a backup option). It explains that if the phone is lost, a backup option is needed. There's a dropdown menu for country selection (Czech Republic is selected). Below that, it asks "Jakým způsobem si přejete získávat kódy?" (How do you want to receive codes?). The "Textová zpráva" (Text message) option is selected with a radio button, and "Telefonní hovor" (Phone call) is unselected. There are "POUŽÍT JINOU ZÁLOŽNÍ MOŽNOST" (Use another backup option) and "ODESLAT" (Send) buttons.

Pokud se žákům objeví tato obrazovka, dokázali nastavit základní 2FA pro účet Google



The screenshot shows the Google 2FA setup screen. At the top, it says "Výzvy od Googlu (Výchozí)" (Google prompts (Default)). Below that, it explains that after entering the password, a prompt will be sent to the phone. There's a "Poznámka" (Note) section: "Poznámka: Pokud se ve způsobem telefonu přihlásíte k účtu Google, začnete dostávat výzvy od Googlu jako další metodu pro dvoufázové ověření." (Note: If you log in to your Google account using your phone, you will start receiving prompts from Google as an additional method for two-step verification). Below the note, there's a section for "Huawei P20 lite" with "Přidáno Neznámé" (Added Unknown) below it. At the bottom, there's a section for "Hlasová zpráva nebo SMS" (Voice message or SMS) with a green checkmark and the text "75 Ověřeno" (75 Verified). Below that, it says "Ověřovací kódy se odesílají prostřednictvím textových zpráv." (Verification codes are sent via text messages). There is a "PŘIDAT TELEFON" (Add phone) button at the bottom.

3) Ověření funkčnosti 2FA (výzvy nebo kódy) – Žáci se odhlásí ze svých účtu --> znovu se přihlásí, aby zkontrolovali funkčnost autentizace.

Zde vidíme příklad přihlášení na PC a výzvy na smartphonu. Žáci mohou vyzkoušet i přihlášení na smartphonu a použití SMS-kódu.

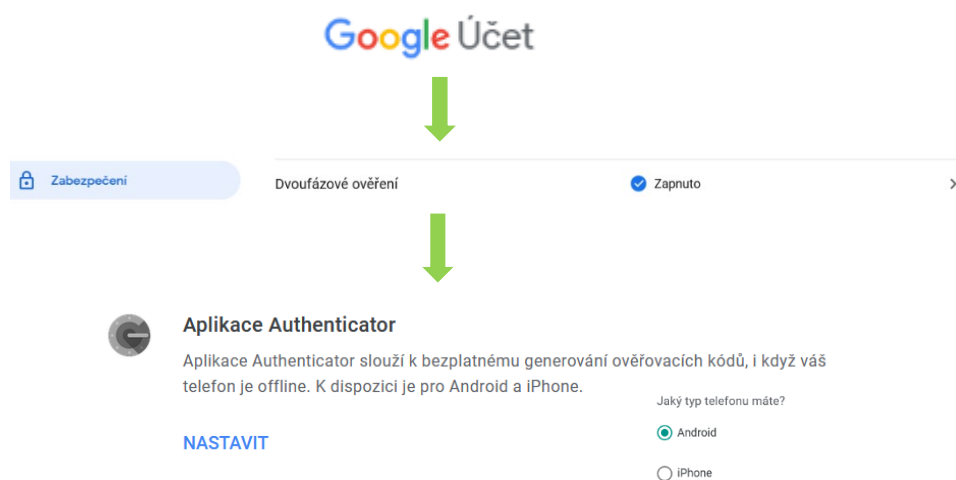
The top part of the image shows a desktop browser window with the Google login page. The user's name 'Filip' and email '@centrum.cz' are visible. A password field contains 'Zadejte heslo'. Below it is a checkbox for 'Zobrazit heslo' and a link 'Zapomněli jste heslo?'. A blue button labeled 'Další' is at the bottom. A red text label 'První faktor - HESLO' is overlaid on the password field. To the right, a green arrow points to a smartphone screen. The phone screen shows a notification: 'Pokoušíte se přihlásit z jiného počítače?' with the user's name and email. It lists device details: 'Zařízení: Windows NT 10.0', 'Oblast: Kevřiná, Česko', and 'Čas: Právě teď'. There are 'NE' and 'ANO' buttons. A red text label 'Druhý faktor - VÝZVA' is overlaid on the notification.

The bottom part of the image shows a desktop browser window displaying the Google account settings page. The header includes 'Google Účet' and a search bar. A list of menu items is shown: 'Přehled', 'Osobní údaje', 'Data a personalizace', 'Zabezpečení', 'Lidé a sdílení', 'Platby a předplatné', and 'Informace'. A red text label 'Úspěšné přihlášení' is overlaid on the left side. A large green checkmark is overlaid on the right side of the menu items.

Pokud žáci v rámci hodiny zvládají nastavit bezpečnostní prvek 2FA pro účet Google, můžeme s nimi hledat odlišnosti v nastavení jednotlivých služeb FB, IG, Twitter, LinkedIn a jiné.

3) Využití aplikace Google Authenticator


Tuto část můžeme pojmut jako nadstavbu našeho tématu bezpečnosti, čímž žáci pronikají hlouběji do problematiky zabezpečení účtů 2FA.



Žáci a studenti mají možnost výběru mezi iPhone a Android. Nainstalují aplikaci Authenticator a nastaví účet pomocí QR kódu do svých zařízení. Pro lepší pochopení aplikace si žáci spustí krátké video, přiložené u aplikace v Google play, popisující její využití. Pokud nelze naskenovat QR, postupujeme dle instrukcí.

Nastavení aplikace Authenticator

- Stáhněte si z [Obchodu Play](#) aplikaci Authenticator.
- V aplikaci vyberte **Nastavit účet**.
- Zvolte **Skenovat čárový kód**.



NEDAŘÍ SE JEJ NASKENOVAT?

Čárový kód nelze naskenovat?

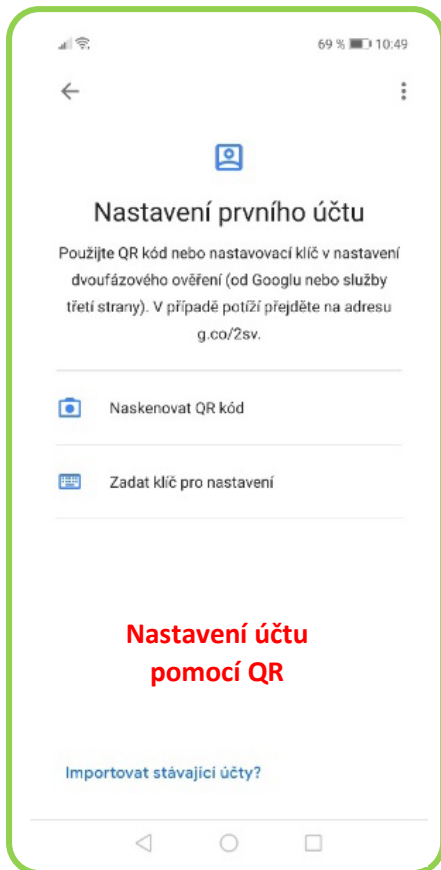
1. Klepněte na **nabídku** a poté na **Nastavit účet**.
2. Klepněte na **Zadat poskytnutý klíč**.
3. Zadejte svou e-mailovou adresu a tento klíč:

Na mezerách nezáleží
4. Zkontrolujte, zda je vybrána možnost **Na základě času**, a klepnutím na **Přidat** proces dokončete.

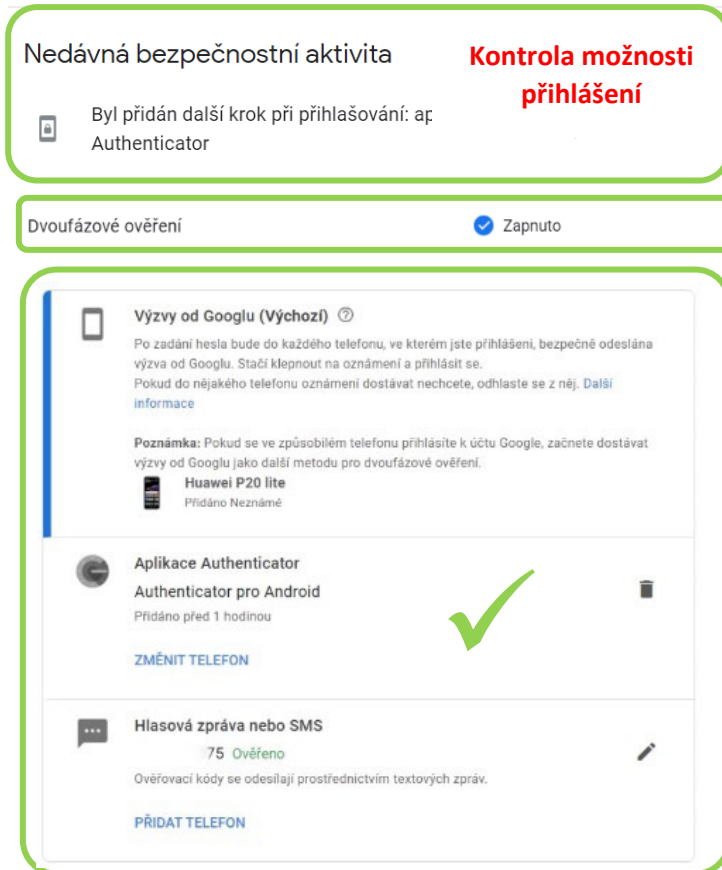
[ZPĚT](#) [DALŠÍ](#)

V dalších krocích žáci pracují se dvěma zařízeními za účelem autentizace přihlášení k účtu Google ve spolupráci s aplikací. Následně si ověří, zda došlo k přiřazení nové možnosti přihlášení k účtu (Nedávná bezpečnostní aktivita).

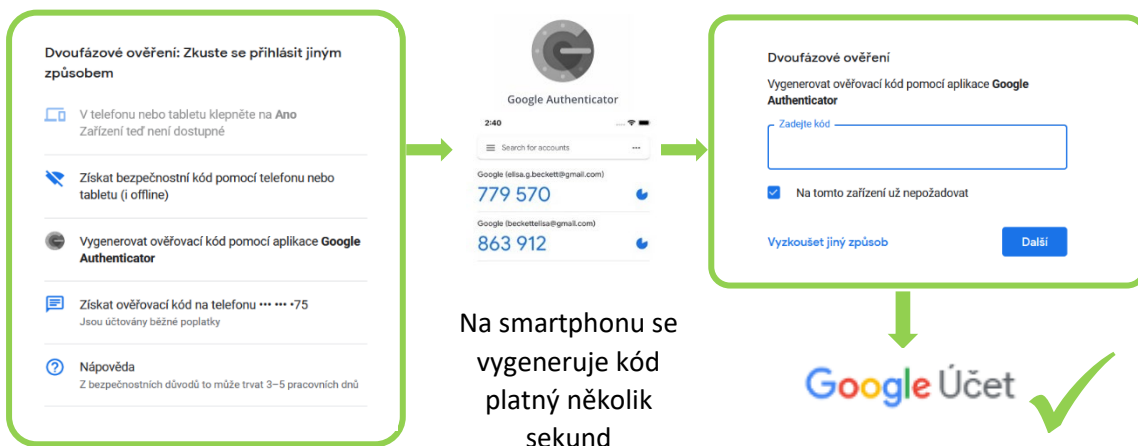
Smartphone



Local



Nyní se žáci odhlásí ze svého účtu Google na počítači či tabletu a vyzkouší si přihlášení pomocí aplikace Authenticator.



Pozn.: Informatika by měla úzce kooperovat s anglickým jazykem a vytvářet mezipředmětové vztahy. Pedagog může využít sdílený prostor pro anglická slovíčka (po celý školní rok popř. pro konkrétní tematický celek), netýká se jen tématu 2FA. Ve sdílené tabulce budou žáci ukládat anglická slovíčka technického, resp. infromatického zaměření. Pokud se jedná o jednoduchý program, je vhodné jej vyučovat v anglické mutaci.

Na co si dát pozor

- Pokud dojde k určitým nesrovnalostem, tak ve většině případů je vše vyřešeno odhlášením a opětovným přihlášením k účtu například nezobrazení telefonu přijímající výzvy.
- Pedagog si, dle náročnosti a šikovnosti žáků, může vybrat jen jednu možnost nastavení 2FA
- V rámci aktualizací Google prostředí se mohou změnit jednotlivé části nastavení

Alternativní řešení

- Dvoufaktorovou autentizaci mohou žáci procvičovat i v účtech sociálních sítí.
- Jako náhradu za Google Authenticator je možno použít například aplikaci Authy, FreeOTP a mnoho jiných, které nalezneme v App Store nebo Google Play.

Zdroje:

- Grafika: autor Filip Szkorupa; zpracování vlastní, prostředí služeb Google [online]. Dostupné z: <https://myaccount.google.com/> a Google Authenticator. *Google Authenticator* [online]. Dostupné z: <https://googleauthenticator.net/>