1. Dvoufaktorové zabezpečení účtů (2FA)

Filip Szkorupa

Oblast z RVP Doporučený stupeň	Digitální technologie 2. stupeň ZŠ, nižší ročníky SŠ
Naplňované výstupy RVP	• 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	• Žáci pochopí princip dvoufaktorové autentizace • Žáci umí nastavit 2FA • Žáci chápou důležitost zabezpečení účtů • Žáci rozvíjí slovní zásobu anglického jazyka
Rozvíjené kompetence	**Kompetence k učení** • Získává hlubší přehled o bezpečnosti vlastních účtů • Experimentuje s různými možnostmi nastavení zabezpečení účtů a posuzuje jejich vhodnost **Kompetence k řešení problémů** • Užívá při řešení problémů logické postupy • Dokáže zvolit efektivní způsob zabezpečení svých účtů **Kompetence komunikativní** • Vysvětlí princip zabezpečení účtu pomocí 2FA • Dokáže popsat důvody zabezpečení pomocí 2FA
Potřebné vybavení	• Zařízení připojené k internetu (PC, Notebook) • Smartphone pro dvoufázové ověřování • Účet Google nebo Apple, účty sociálních sítí • Aplikace 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.

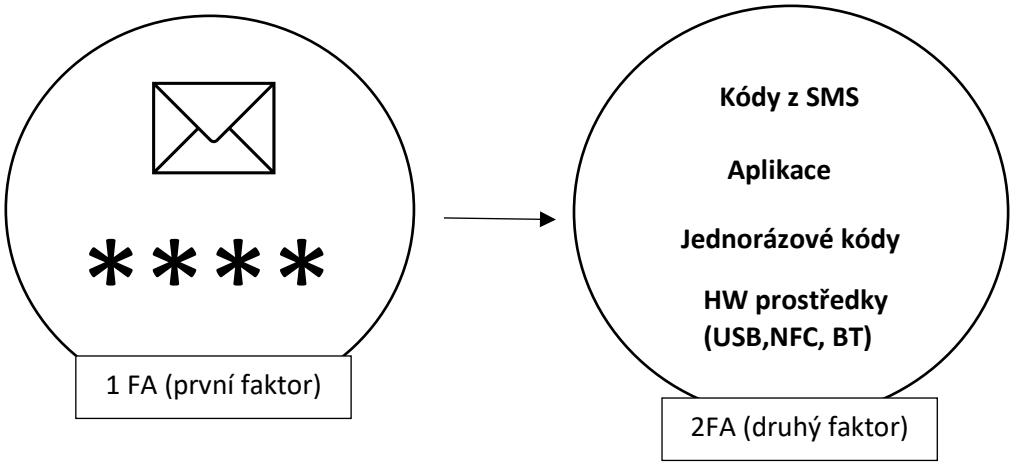
Otázka na žáky: Jaké formy zabezpečení používáte na svých účtech?

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.

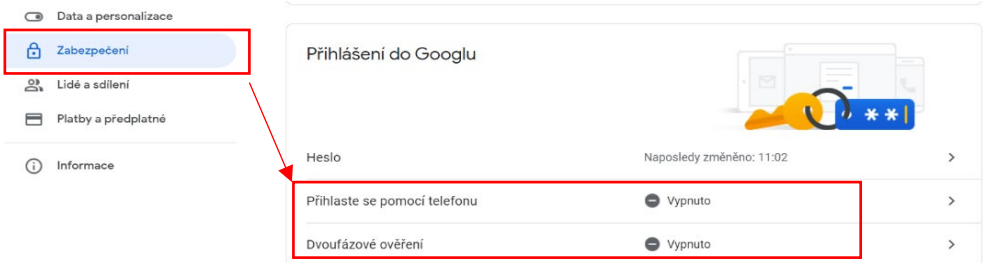
Pokusíme se s žáky nastavit různé možnosti zabezpečení 2FA:

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

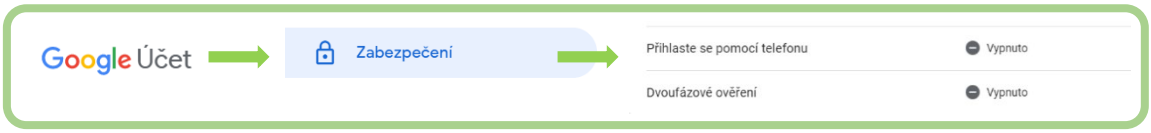
Pedagog si, dle náročnosti a šikovnosti žáků, může vybrat jen jednu možnost. Samotná aktivita žáků probíhá na školních počítačích, vhodné je také zařazení BYOD, resp. si to následující činnosti přímo vyžadují.

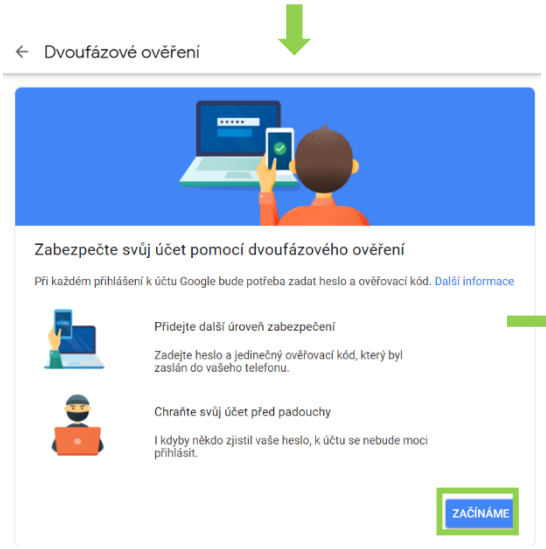
Postup nastavení 2FA

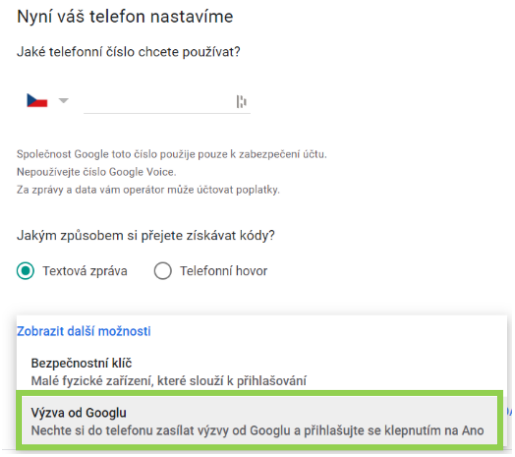
1) Žáci se přihlásí ke svým účtům a zapnou dvoufázové ověření



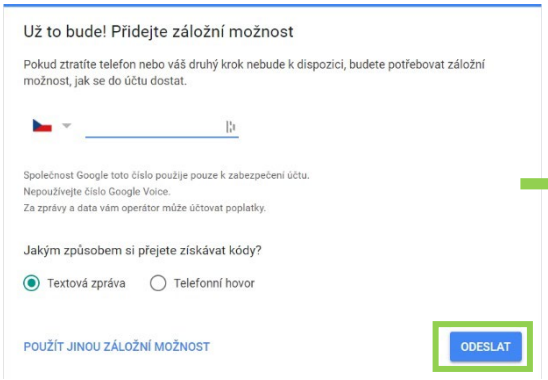
2) S žáky nastavíme zabezpečení pomocí **výzev (jednorázových kódů)**, které uživatel dostává na telefon (Android, iOS) přihlášený k účtu. Nastavení je velmi intuitivní. Se žáky postupujeme krok za krokem, v případě obtíží individuálně řešíme komplikace například nezobrazení mobilního zařízení, na které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

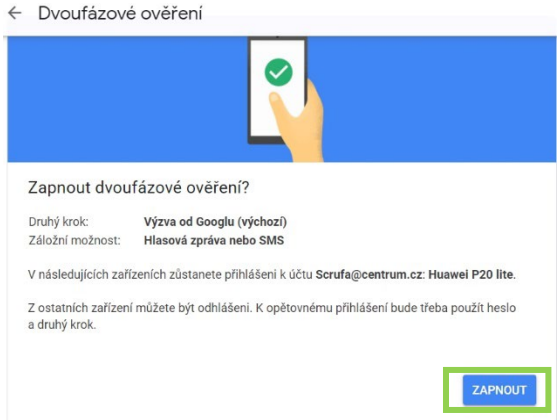




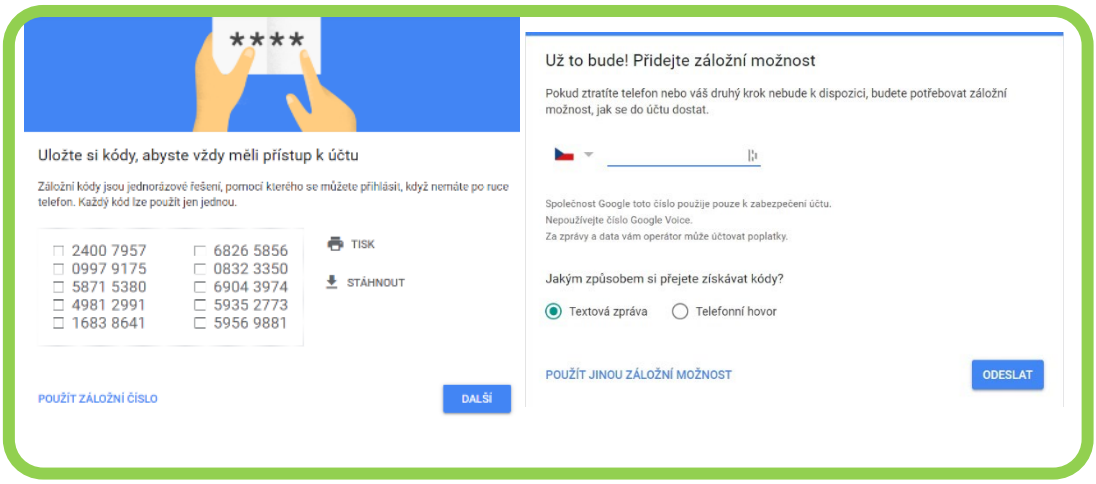


Může nastat komplikace – uživatel musí nastavit svůj účet na telefonu

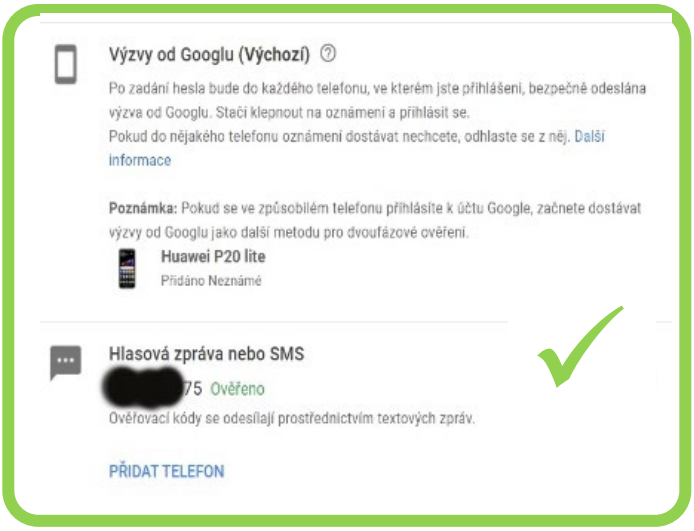




V další části můžeme s žáky nastavit alternativní možnosti přihlášení pomocí jednorázových kódu nebo telefonního hovoru.

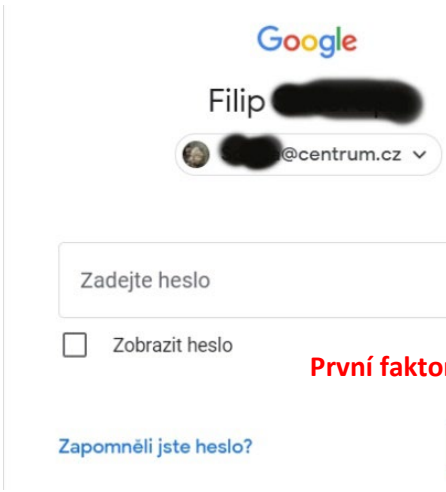


Pokud se žákům objeví tato obrazovka, dokázali nastavit základní 2FA pro účet Google

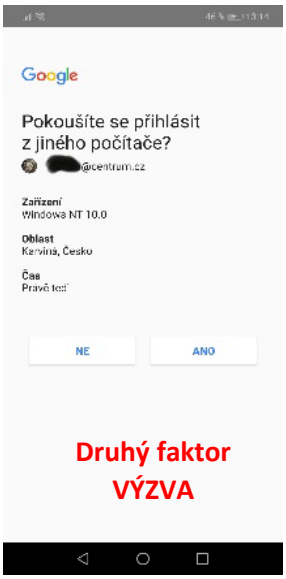


3) Ověření funkčnosti 2FA (výzvy nebo kódy) – Žáci se odhlásí ze svých účtu --> znovu se přihlásí, aby zkontrolovali funkčnost autentizace.

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

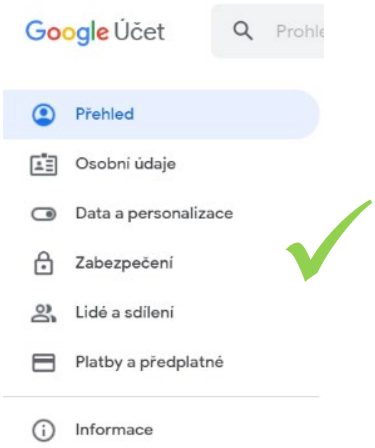


První faktor - HESLO



Druhý faktor
VÝZVA

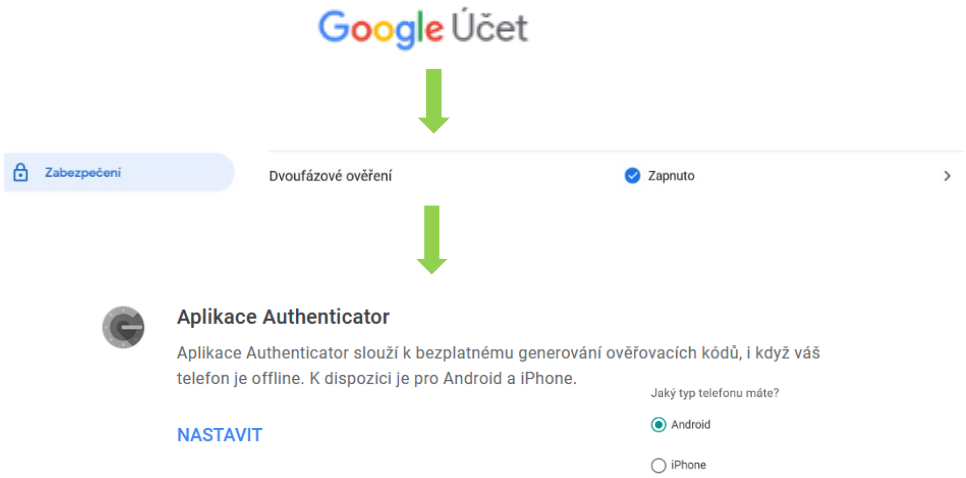
Úspěšné přihlášení



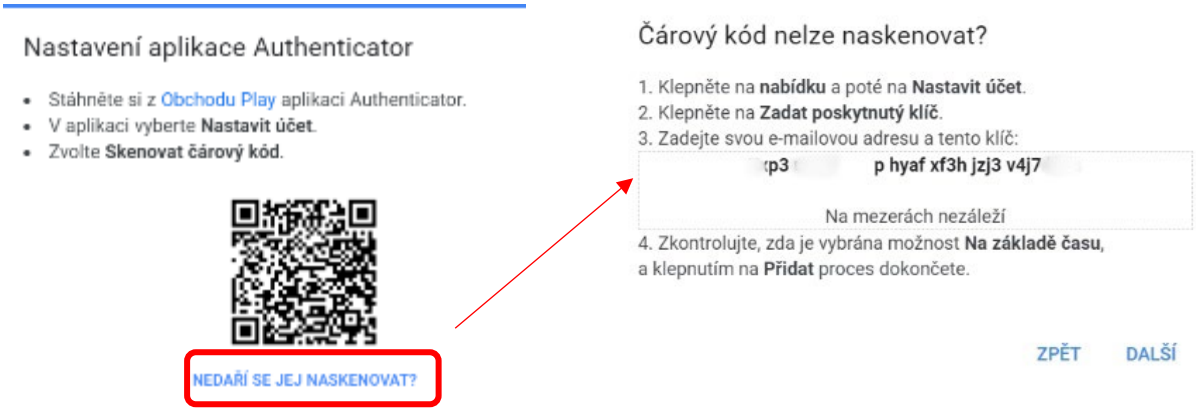
Pokud žáci v rámci hodiny zvládají nastavit bezpečnostní prvek 2FA pro účet Google, můžeme s nimi hledat odlišnosti v nastavení jednotlivých služeb FB, IG, Twitter, LinkedIn a jiné.

3) Využití aplikace Google Authenticator

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

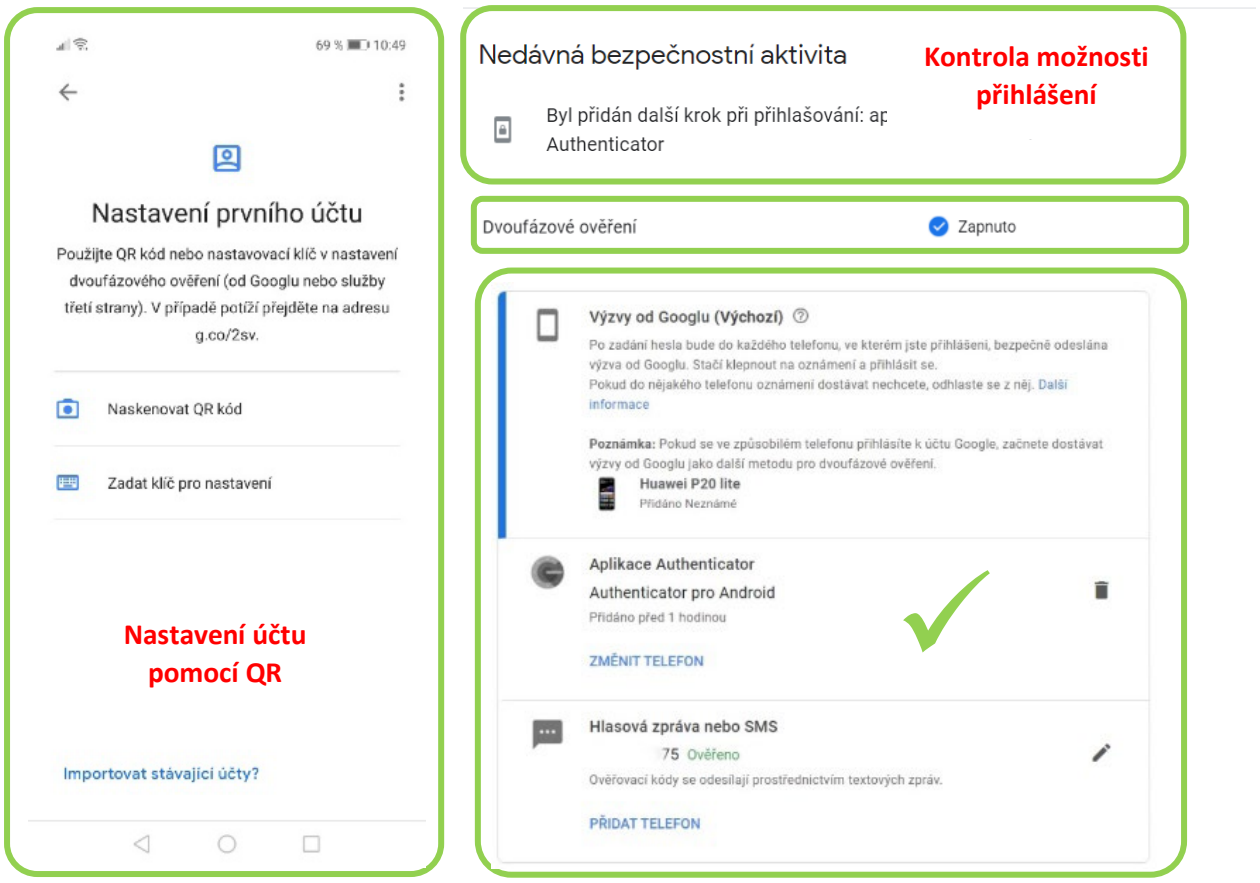


Žáci a studenti mají možnost výběru mezi iPhone a Android. Nainstalují aplikaci Authenticator a nastaví účet pomoc QR kódu do svých zařízení. Pro lepší pochopení aplikace si žáci spustí krátké video, přiložené u aplikace v Google play, popisující její využití. Pokud nelze naskenovat QR, postupujeme dle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

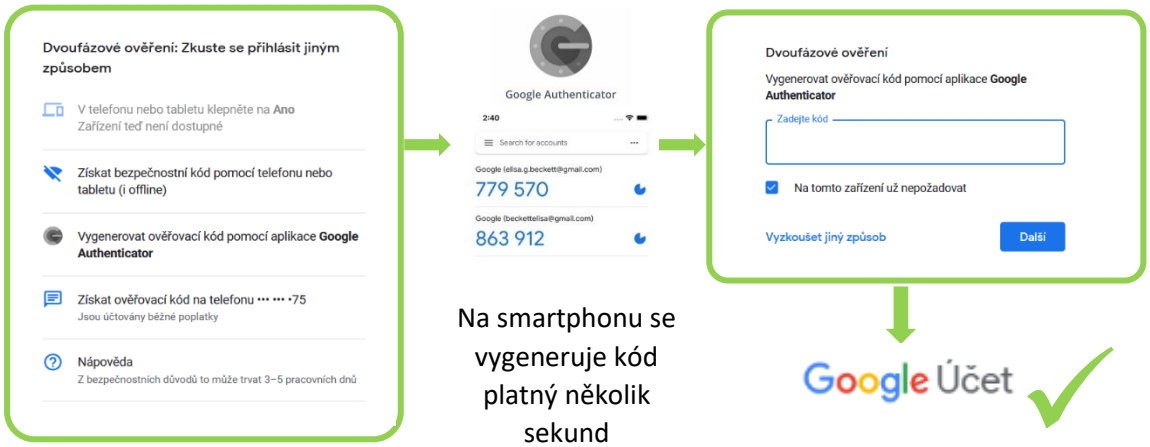


V dalších krocích žáci pracují se dvěma zařízeními za účelem autentizace přihlášení k účtu Google ve spolupráci s aplikací. Následně si ověří, zda došlo k přiřazení nové možnosti přihlášení k účtu (Nedávná bezpečnostní aktivita).

Smartphone **Local**



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



Na smartphonu se vygeneruje kód platný několik sekund

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. informatického 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/