

## Téma: Trestné činy proti ochraně informací

### Aktivita

<b>Cíl</b>	Aktivita pomůže naučit se / upevnit si návyky / metody související s používáním dvou faktorové autentizace (2FA).
<b>Doba trvání</b>	Přibližně 30 minut
<b>Cíle</b>	Zjistit, jaké jsou znalosti účastníků o používání dvou faktorové autentizace. Uvést, jaké jsou výhody používání těchto bezpečnostních opatření. Ukázat, jak povolit / aktivovat dvou faktorovou autentizaci na příkladu Allegra / Facebook / Internet mail / ePUAP.
<b>Potřebné pomůcky</b>	Telefon/tablet/počítač s připojením k Internetu, papír, karty aktivit, tabule, psací potřeby
<b>Instrukce</b>	<ul style="list-style-type: none"><li>– Požádejte účastníky, aby si na své karty napsali příklady dvou faktorové autentizace (dvoufázové ověření), pokud daný pojem znají nebo s čím jej spojují, např. jednorázové kódy nebo odkazy zaslané e-mailem, jednorázové kódy zaslané SMS, časové kódy v aplikaci dongle</li><li>– Poskytněte tipy, jak povolit dvoufázové ověření přístupu k různým účtům</li><li>– Požádejte účastníky, aby napsali své příklady z kartiček na tabuli a označili místa, kde se vyplatí tento typ zabezpečení použít (např. webové stránky banky, aukční web, e-mailový účet, sociální síť)</li><li>– Proveďte skupinovou diskusi o použití dvou faktorové autentizace a výhodách a nevýhodách použití konkrétních bezpečnostních metod, může být formou společného vyplňování tabulky</li></ul>

## Vzorová tabulka pro aktivitu

Dvoufázová metoda ověření	Výhody	Nevýhody
jednorázové kódy nebo odkazy zaslané e-mailem		
jednorázové kódy zaslané SMS		
časové kódy v aplikaci		
U2F dongle		
biometrie – obličej, hlas, otisk prstu		

### Doplňující informace:

- může zachytit, přesměrovat
- musíte sdílet své telefonní číslo
- dodatečné náklady
- snadné použití / konfigurace
- odolný vůči phishingovým útokům
- zranitelný vůči phishingovému útoku
- musí být online
- zařízení musí být nabitě / dostupné