Идеи и съвети

Изградете добри навици за безопасност при работа с интернет с помощта на дадените по-долу идеи и съвети. Този раздел е изготвен в сътрудничество с „Get Safe Online“ (Обединено кралство) и Министерството на вътрешната сигурност на Съединените щати.

- Защитете вашия персонален компютър и преносими устройства;
- Защитете вашата лична информация и самоличност;
- Защитете служебната информация, когато сте извън вашата организация;
- Бъдете предпазливи, когато се свързвате с интернет;
- Ползвайте интернет разумно.

Защитете вашия персонален компютър и преносими устройства

Персонални компютри

- Използвайте софтуер „защитна стена“: защитните стени предпазват вашата мрежа от някои вируси и хакерски атаки.
- Инсталирайте антивирусен софтуер: антивирусният софтуер предпазва вашия компютър от разпространение на компютърни вируси.
- Винаги изтегляйте най-новите актуализации на данните за сигурност: поддържайте вашите приложения и оперативна система годни, изправни и актуални.
- Не допускайте проникване на софтуер за шпиониране (спайуер): не позволявайте на непознати да получават достъп до компютъра ви, като избягвате да отваряте подозрителни електронни писма и прикачени файлове към тях.
- Редовно правете резервни копия на вашите данни, за да можете да ги възстановите в случай на технически проблем.

Преносими компютри (лаптопи)

- Изключвайте безжичните връзки, когато не ги използвате или не са необходими.
- Редовно свързвайте вашия лаптоп към надеждна мрежа, за да актуализирате вашите инструменти за сигурност.
- Правете резервни копия на информацията, съхранявана във вашия лаптоп;
- Не оставайте вашия лаптоп без наблюдение.

Флаш памети с интерфейс USB

- Използвайте криптирана USB флаш памет.
- Конфигурирайте с помощта на физическия превключвател USB флаш паметта в режим, допускащ само четене на информацията, за да избегнете разпространението на

вируси: някои USB флаш памети са оборудвани с физически превключвател за активиране на режим, допускащ само четене на информацията, който не позволява запис или промяна на данните във флаш паметта от компютъра.
- Сканирайте флаш паметта след копиране на файлове от компютър, който не считате за надежден и/или който не е одобрен.
- Преди да включите вашата флаш памет в чужд компютър, изтрийте всички файлове, които не са свързани с целта на това действие.
- Изготвяйте резервни копия на информацията, съхранявана на вашата флаш памет, за да можете да я възстановите в случай на технически проблем.
- Прикрепяйте USB флаш паметта към ключодържател/връв, за да предотвратите изгубване на информационния носител: малките размери на USB флаш паметите са предпоставка за по-лесно изгубване или кражба на тези устройства. Освен това, с оглед на увеличения капацитет за съхранение на информация, нараства и потенциалният обем на данните, които са застрашени от нерегламентиран достъп. USB флаш паметите често се пренасят в чанти, раници, калъфи за преносими компютри, джобове на горни дрехи и панталони, или биват оставяни без наблюдение, когато са включени към компютри на работните места. Напоследък нараства броят на инцидентите, свързани с изгубване, неправилно съхранение, използване без разрешение или кражба на USB флаш памети.

Мобилни телефони и джобни компютри

Джобните компютри като Windows Mobile, Palm, iPhone, Android и Blackberry са оборудвани с възможности за връзка с интернет и с капацитет за съхранение на големи обеми данни. Преносимостта на тези устройства предполага, че към тях трябва да се подхожда с особена предпазливост.

- Изключвайте безжичните връзки (например Bluetooth или WLAN), когато не ги използвате. Технологията Bluetooth позволява на електронни устройства да комуникират помежду си с помощта на радиовръзка с малък обхват.
- Не оставяйте без наблюдение вашия мобилен телефон или джобен компютър. Неспазването на това правило може да доведе до загуба на данни.
- Използвайте функцията за контрол на достъпа чрез парола, за да предотвратите неразрешен отдалечен достъп до вашия смартфон.

Защитете вашата лична информация и самоличност

- **Използвайте трудна за отгатване парола**: вашата парола е еквивалентът в интернет на ключалката и ключа, с чиято помощ защитавате дома си. Използването на пароли е ефективна предпазна мярка и възприемането на добри практики за използване на пароли ще способства за сигурността на вашата чувствителна лична информация и самоличността ви. Паролата за отваряне на вашия компютър е ключът за достъп до

цялата служебна и лична информация, която съхранявате в паметта му и в уебсайтове, в които имате регистрация (акаунт). Използвайте трудна за отгатване парола, за да защитите вашите данни: паролата трябва да е сложно съчетание от знаци; комбинирайте букви (главни и малки), цифри и символи. Колкото по-разнообразни знаци включва вашата парола, толкова по-трудно е тя да бъде отгатната. Не използвайте лична информация — вашето име, име на член на семейството ви, рождени дати и т. н., която някой може да знае или да получи лесно, а също така се старайте да избягвате думи от речта: някои хакери използват програми, които въвеждат в полето за парола последователно всички думи, съдържащи се в речника.

- **Сменяйте редовно вашата парола**: ако имате основания да смятате, че е осъществен неразрешен достъп до вашата система, сменете незабавно паролите, които използвате.
- **Пазете в тайна вашата парола**: вашата парола е уникална и не бива да я споделяте с никого. Ако е възможно, старайте се да запомняте вашите пароли. Изградете си стратегия за тяхното запаметяване. Ако си записвате използваните пароли, внимателно обмисляйте къде да съхранявате записките. Не ги съхранявайте на места, където не бихте оставили информацията, която защитават съответните пароли.
- **Уникална парола за всеки онлайн акаунт**: използвайте различна парола за достъп до всеки онлайн акаунт (или поне няколко различни пароли). Ако използвате една и съща парола за достъп до различни акаунти, хакер, който успее да пробие защитата на един акаунт, ще получи достъп до всички ваши акаунти.
- **Използвайте допълнителна защита за вашите акаунти**: много уебсайтове, които изискват регистрация за ползване на предлаганите от тях услуги, прилагат допълнителни способи за удостоверяване на вашата самоличност, за да ви предоставят достъп до вашия акаунт.
- **Контролирайте вашето присъствие в мрежата**: когато е възможно, регулирайте настройките за защита на личните данни и сигурност на посещаваните уебсайтове, така че да контролирате обхвата на информацията, която споделяте. Препоръчително е да ограничавате кръга на лицата, с които споделяте информация.
- **Използвайте внимателно т. нар. социални мрежи**: имайте предвид, че сайтовете на социалните мрежи могат да съчетаят на едно място много от рисковете, свързвани с присъствието в интернет: отправяне на заплахи онлайн, неразрешен достъп до лични данни, кибертормоз, достъп до неподходящо с оглед възрастта на потребителя съдържание и в най-тежките случаи сприятеляване с цел сексуална злоупотреба и сексуално насилие над деца.

Защитете служебната информация, когато сте извън вашата организация

- **Съхранявайте сигурно чувствителната информация**: когато сте извън вашата организация, уверете се, че сте предприели мерки за гарантиране сигурността на чувствителната информация и комуникационното оборудване, за да предотвратите

кражба или загуба на данни. По-специално, когато сте на публични места, подхождайте с внимание към опазването на информацията.

- **Гарантирайте поверителния характер на служебната информация**: имайте предвид, че някой може да подслуша разговора ви. Не предоставяйте на никого поверителната информация на вашата организация.
- **Пазете се от странични погледи**: когато пътувате или осъществявате достъп до вашите данни чрез интернет, предпазвайте данните от погледите на странични наблюдатели.
- **Използвайте предпазливо електронната си поща чрез уебстраници**: използването на интернет браузер за четене на вашата електронна поща предполага аналогична степен на внимание, както и десктоп програмите за електронна поща, като освен това е свързано с няколко риска, характерни конкретно за този способ за достъп до електронна кореспонденция.

Бъдете предпазливи, когато се свързвате с интернет

- **Изключвайте безжичните връзки, когато не ги използвате или не са необходими.**
- **Бъдете предпазливи при използване на Wi-Fi „горещи точки“**: Когато използвате Wi-Fi горещи точки, ограничавайте дейностите, които извършвате онлайн, и коригирайте настройките за сигурност на вашето устройство, за да ограничите кръга на лицата, които имат достъп до него.
- **Защитавайте вашите пари:** когато извършвате банкови операции или пазарувате онлайн, се уверявайте, че съответните уебсайтове поддържат защитен обмен на данни. Проверявайте дали адресите на сайтовете започват със символните комбинации „https://“ или „shttp://“, което означава, че съответният сайт прилага допълнителни мерки, за да гарантира сигурността на вашата информация. Сайтовете, чиито адреси започват със символите „http://“, не са защитени.
- **Не приемайте нежелани електронни съобщения**: Спам съобщенията са заплаха за сигурността. Не отваряйте електронни писма и приложения към тях с неизвестен подател.
- **Не отваряйте връзки, които ви изглеждат съмнителни**: когато хипервръзки, които се съдържат в електронни писма, съобщения в Туитър, публикувани мнения и онлайн реклами, ви изглеждат подозрителни, дори подателят им да ви е известен, е най-добре да ги изтриете или, ако е уместно, да ги маркирате като спам.
- **Препращайте електронните писма, когато е уместно**. Обмислете дали да изтриете историята на писмото, преди да го препратите.
- **Сърфирайте в интернет внимателно.**
- **Не отваряйте документи и други материали, предоставени от податели, на които нямате доверие.**
- **Използвайте внимателно компютри за обществено ползване:** свързвайте се с интернет от компютри за обществено ползване, само когато разполагате с криптирана връзка (обозначена с иконка във формата на катинар в долния десен ъгъл на

прозореца на браузера, както и със съчетанието от символи „https://“ в началото на адреса на уебсайта).

- **Използвайте услуги за уеб електронна поща, предоставяни само от известни и надеждни компании.**

Ползвайте интернет разумно

- **Бъдете информирани:** осведомавявайте се за новите начини за обезпечаване на вашата сигурност онлайн: проверявайте уебсайтове, на които имате доверие, за актуална информация, и споделяйте тази информация със семейството, приятелите и колегите си, като ги насърчавате да използват интернет разумно. Уверете се, че вашият интернет браузер е защитен.
- **Мислете, преди да действате**: подхождайте внимателно към съобщения, които ви приканват да действате незабавно, съдържат предложение, което изглежда твърде примамливо, за да е истинско, или искане да предоставите свои лични данни.
- **Правете резервни копия на вашите файлове**: предпазвайте вашата служебна информация, музикални файлове, снимки и други цифрови данни, като изготвяте и съхранявате сигурно архивни копия на файловете.