Capes de seguretat: contrasenya, firewall, antivirus, còpies.

DIGITALITZACIÓ · 4t ESO

UNITAT 4: SEGURETAT DIGITAL

Nom: _____ Curs/Grup: _____ Data: _____

Durada: 12 sessions. Al final sabràs:

- Identificar riscos, amenaces i atacs als dispositius i a la xarxa.
- Configurar mesures de protecció: contrasenyes, antivirus, actualitzacions.
- Protegeir les dades personals, la petjada digital i la identitat a la xarxa.
- Configurar correctament la privadesa en apps i xarxes socials.

SESSIÓ 1-2 · Riscos i amenaces: què ens pot passar

> *DEFINICIÓ: Amenaça = situació o agent que pot danyar els teus dispositius, dades o béestar. Risc = la possibilitat que passa.*

Classificació de les amenaces més habituals:

Amenaça
Malware (virus, troians)
Phishing
Ransomware

Adware/spyware
Enginyeria social
Atac de força bruta

Idea clau: el 95% dels atacs comencen per un ERROR HUMÀ: clicar un enllaç, una contrasenya feble, confiar en algú que se suposa de confiança. La tecnologia ajuda, però la primera defensa ets tu.

Activitat 4.1 — Classifica les amenaces (grups)

Llegeix aquests 5 casos reals i identifica quina amenaça és cada un:

- A. 'M'ha arribat un SMS de La Caixa demanant-me les credencials del compte.'
- B. 'Un programa que he instal·lat em surt publicitat cada 2 minuts.'
- C. 'He obert un fitxer d'un correu d'un desconegut i ara tots els meus documents han canviat d'extensió.'
- D. 'Alguns coneixen la meva contrasenya perquè és el nom del meu gos.'
- E. 'He rebut una trucada: 'sóc Microsoft, tens un virus, connecta'm al teu PC'.'

1. _____ 2. _____ 3. _____ 4. _____ 5. _____

La contrasenya és el candau dels teus comptes.

SESSIÓ 3-4 · Contrasenyes i autenticació

> *DEFINICIÓ: Autenticació de dos factors (2FA): a més de la contrasenya, cal un segon element (codi al mòbil, empremta) per entrar.*

Contrasenyes fortes

- Llargues: mínim 12-16 caràcters (cada caràcter extra complica exponencialment).
- Variades: majúscules, minúscules, números, símbols.
- Úniques: una contrasenya diferent per a cada servei important.

- NO personals: res de dates de naixement, noms de familiars o mascotes.

TÈCNICA de frase-contrasenya: 'Corre-3-Gats-Pluja-2026' és llarga, fàcil de recordar i difícil de forçar.

El gestor de contrasenyes

Memoritzar 30 contrasenyes úniques és impossible. La solució professional és un gestor: guarda totes les contrasenyes xifrades i tu només recordes una contrasenya mestre. Opcions: Bitwarden (gratuït i lliure), KeePass, el gestor del navegador o del mòbil.

Autenticació de dos factors (2FA)

- Alguna cosa que SABS (contrasenya) + alguna cosa que TENS (codi al mòbil).
- Fins i tot si roben la contrasenya, sense el segon factor no entren.
- Activa-la SEMPRE a: correu, banc, xarxes socials, Instagram/TikTok.

Activitat 4.2 — Audita les teves contrasenyes (individual)

1. Quants serveis importants uses amb contrasenya? (correu, xarxes, banc, escola...)

Número aproxim: _____

2. Quants d'ells usen la MATEIXA contrasenya? _____

3. Prova el test de la tècnica frase-contrasenya: escriu una frase i converteix-la:

Frase: _____ Contrasenya resultant: _____

4. El 2FA està actiu en: correu? ____ Banc? ____ Xarxes? ____

SESSIÓ 5-6 · Protecció dels dispositius

Capa de protecció 1: el sistema actualitzat

Cada actualització del SO tapa forats de seguretat descoberts. Un sistema sense actualitzar és una porta oberta. Regla: actualitza SIEMPRE, el mateix dia si es pot.

Capa de protecció 2: antivirus / antimalware

Eina
Windows Defender
Antivirus de pagament
Firewall
Sentit comú

Capa de protecció 3: còpies de seguretat

> *REGLA 3-2-1: 3 còpies de les dades, en 2 suports diferents, 1 d'elles fora de casa (núvol).*

Si t'ataquen amb ransomware, la única defensa real és tenir còpia: no pagues rescat, restaures i ja hi ets.

Capa 4: bloqueig i xifrat

- Bloqueig de pantalla amb PIN/biometria sempre actiu.
- Xifrat del disc (BitLocker a Windows, FileVault a Mac, LUKS a Linux): si roben l'equip, no llegiràn les dades.
- Bloqueig remot: localitzar i esborrar un mòbil perdut (Find My Device).

Activitat 4.3 — Auditoria de seguretat del teu dispositiu (1h)

Revisa el teu mòbil o un PC del taller i marca el que comprovis:

Comprovació
SO actualitzat
Antivirus actiu (o Defender)
Bloqueig de pantalla actiu
Còpia de seguretat recent
2FA en el correu
Gestor de contrasenyes

Conclusions de l'auditoria (què has de millorar?):

_____

SESSIÓ 7-8 · Privadesa i petjada digital

> *PETJADA DIGITAL: el rastre de dades que deixes a Internet (posts, cerques, ubicacions, compres, 'likes').*

La petjada és PERMANENT: el que puges avui el poden veure d'aquí 10 anys (universitats, empreses). Internet no oblida.

Configuració de privadesa

- Revisa qui pot veure els teus posts (públic? amics? personalitzat?).

- Desactiva la publicitat personalitzada on es pugui.
- Revisa els permisos d'apps: per què una llanterna demana la ubicació?
- Draughts: elimina apps que no uses i les seves dades.
- Cerca't a Google (nom + cognom): què hi ha de tu? És el que vols que es vegi?

Identitat digital

La teva identitat digital és el que els altres perceben de tu a la xarxa. Construeix-la: posts que poguessin veure els teus pares o un professor sense avergonyir-te; no publiquis ubicació en temps real; no comparteixis fotos de tercers sense permís.

Activitat 4.4 — Auditoria de privadesa (individual)

1. Cerca't a Google: nom + cognom + població. Què surt?

_____

2. Revisa els permisos de 5 apps del teu mòbil. Quina app té permisos que no necessita?

_____

3. Revisa la configuració de privadesa d'Instagram/TikTok: qui veu els teus posts?

_____

SESSIÓ 9-10 · Resposta a incidents

Què fer si ja t'ha passat?

Situació
He clicat un enllaç phishing i he posat dades
El PC va estrany (lent, pop-ups)
M'han robat el mòbil
M'han suplantat la identitat a la xarxa
He rebut ciberassetjament

Activitat 4.5 — Anàlisi de phishing real (parells)

El professor mostrarà 5 correus/SMS (uns legítims, uns falsos). Per a cada un:

Legítim o phishing? Per què? Quins indicadors has vist?

1. _____ Indicadors: _____
2. _____ Indicadors: _____

3. _____ Indicadors: _____
4. _____ Indicadors: _____
5. _____ Indicadors: _____

Indicadors tipus de phishing: remitent estrany, salutació genèrica, urgència falsa, enllaç que no coincideix amb el text visible, errors d'ortografia, demana dades sensibles.

Repàs i autoavaluació

Rúbrica: 1 = No assolit · 2 = Satisfactori · 3 = Notable · 4 = Excel·lent

Objectiu
Identifico les principals amenaces digitals i els seus indicadors
Uso contrasenyes fortes, úniques i 2FA
Sé configurar protecció bàsica d'un dispositiu (actualitzacions, bloqueig, còpies)
Sé què és la petjada digital i com gestionar la meva identitat en línia
Sé què fer davant un incident de seguretat

Glossari

- Malware: programa maliciós (virus, troià, spyware).
- Phishing: suplantació per robar credencials.
- Ransomware: malware que xifra fitxers i demana rescat.
- 2FA: autenticació de dos factors.
- Gestor de contrasenyes: aplicació que guarda contrasenyes xifrades.
- Còpia 3-2-1: 3 còpies, 2 suports, 1 fora de casa.
- Petjada digital: rastre de dades que deixes a la xarxa.
- Enginyeria social: manipulació psicològica per obtenir dades o accés.