COMPRÉHENSION ORALE

LES CAMERAS ONT DES YEUX

CORRIGÉS

1. Sur les risques réels de hacking des caméras

2. Facile

3. Ils allument la webcam

4. Récupérer des informations compromettantes pour les vendre

5. Il n'y a pas une cible principale

6. Les camarades de classe

7. Deux réponses parmi : Dans un but de harcèlement OU Dans un but pervers OU Dans le but de les observer chez eux

8. C'est une demande de rançon. On demande de l'argent en échange de vidéos ou photos ou autres fichiers compromettants, par exemple, dans des moments intimes qu'une personne ne veut pas voir distribués.

9. La compétition.

10. Trois réponses parmi : Faire attention à ce que l'on installe sur nos appareils / Faire attention à là où on clique / Avoir un antivirus / Avoir un firewall

11. Il faut le décoller puis le recoller à chaque utilisation de la caméra.

12. La lumière de la caméra.

13. FAUX. Justification : Le son est fait de vibrations, donc, même avec du double ou triple scotch, les vibrations de l'air passent quand même.

14. Cinq réponses parmi : - la télévision – l'interphone d'une porte d'entrée – la tablette – l'ordinateur – le smartphone – la domotique

15. Brancher un fil coupé.

16. Sectionner le micro dans le téléphone.

17. Qu'on ne peut plus rien faire avec.

18. Avec du scotch

TRANSCRIPTION

Animateur : – Vous l'aurez peut-être remarqué au bureau ou dans les cafés, on voit de plus en plus de gens protéger les webcams de leur laptop. Didier Bonvin, vous vous êtes interrogé sur les risques réels de hacking de caméra.

Didier Bonvin : – Oui et j'ai posé la question à un spécialiste, Steven Mayer, CEO et co-fondateur de l'entreprise de cybersécurité genevoise ZenData. Il m'a expliqué que hacker une webcam ou le micro d'une tablette était assez facile, donc pour lui les risques sont bien réels.

Steven : – Malheureusement, c'est une menace assez réelle. On se rend compte qu'il y a une grande quantité de virus et de chevaux de Troie, lorsqu'ils s'installent sur des ordinateurs, ils essaient d'activer la

webcam pour pouvoir espionner la personne derrière l'ordinateur et même d'utiliser le micro pour pouvoir entendre ce que la personne dit afin de pouvoir ensuite monétiser l'information qu'ils récupèrent.

Animateur : – Qui est visé ? C'est Monsieur et Madame tout le monde ? Les entreprises ?

Steven : – Alors oui, c'est exactement tout le monde. On voit trois catégories qui se dessinent principalement : on a tous les jeunes et adolescents qui se font viser souvent par leurs amis ou camarades de classe. Et ça, c'est dans un but plutôt pervers ou dans un but de harceler ou d'observer leurs camarades à la maison. Ensuite, on a toutes les personnes qui sont plus les privées, où là, on rentre dans le crime organisé, où on a typiquement comme le ransomware.

Animateur : – Les demandes de rançon ?

Steven : – Les demandes de rançons exactement : les gens ont leur webcam qui s'est activée et qui se font attraper pendant des moments intimes, ensuite se font menacer : demande de rançon pour éviter de publier ses informations sur le web. Et finalement, après, on a les entreprises ou les politiciens et là, c'est de l'espionnage industriel ou de l'espionnage étatique où ils essaient de récupérer des informations sur leur adversaire ou concurrent.

Animateur : – Alors comment bien se protéger, un simple scotch suffit pour la caméra ?

Steven : – Alors oui un simple scotch peut suffire. De nouveau, comme on dit toujours, il faut avoir une bonne hygiène digitale, faire attention à ce que l'on installe sur nos appareils. Attention là où on clique, avoir un anti-virus, un firewall. C'est vrai que pour la webcam si on met un scotch dessus, ben si la webcam ne voit rien, elle peut pas filmer grand-chose. Après évidemment, c'est pas ce qu'il y a de plus pratique si vous utilisez la webcam régulièrement, il existe même des petits clapets que l'on peut mettre dessus qui sont tout fins, on peut ensuite ouvrir et fermer. Définitivement, c'est quelque chose qui permet d'empêcher la webcam de fonctionner correctement, d'autant plus qu'on sait que lorsqu'une webcam s'active généralement, il y a une petite lumière à côté qui s'illumine, mais les hackers ont réussi à contourner ce système et faire qu'il y a même pas de lumière qui s'allume lorsque la webcam est activée donc la couvrir physiquement, c'est une bonne solution.

Animateur : – Et le micro c'est la même chose ? Un scotch suffit ou il faut faire plus de choses pour se protéger du hacking sur le micro de son laptop ou d'une tablette ou de son smartphone ?

Steven : – Alors le micro, malheureusement, ça ne fonctionne pas avec le scotch. Même si on met un double ou un triple scotch, les vibrations de l'air passent quand même. Donc ça, ça suffit pas et en plus, les micros, on en a beaucoup plus que ce qu'on pense autour de nous. Parce que comme vous avez dit, il y a l'ordinateur, la tablette, le smartphone mais aussi les téléviseurs, la domotique à la maison même l'interphone d'une porte d'entrée ont tous des micros, on est vraiment entourés d'énormément de micros dans notre quotidien et c'est quelque chose auquel il faut faire attention ou en tout cas, se poser la question de « qu'est-ce qu'on peut dire autour d'un micro ? ».

Animateur : – Alors, comment faire si un scotch ne suffit pas ?

Steven : – Sur un ordinateur, vous avez souvent des prises jack ou sur un téléphone, vous avez souvent la prise jack sur laquelle on peut brancher des écouteurs donc si vous branchez un écouteur sectionné ou un micro sectionné dans cette prise jack, c'est une bonne façon d'empêcher un hacker d'écouter votre micro. Ensuite, si vous voulez vraiment rentrer dans la partie extrêmement paranoïaque, on peut suivre les recommandations d'Edward Snowden qui avait dit qu'il fallait carrément couper le micro à l'intérieur de l'appareil téléphonique du smartphone et ensuite n'utiliser qu'un kit mains-libres au moment où vous voulez parler.

Animateur : – D'accord, pour les espions ou hackers.

Steven : – Voilà, exactement. Si on veut une façon qui est pas trop… ou qui ne modifie physiquement la machine, qu'on ait pas quelque chose de visible qu'on est en train de mettre dans la machine, pour les ordinateurs Windows, il y a une technique qui est relativement simple, qui marche dans la majorité des cas. C'est très facile, il suffit d'aller dans le panneau de configuration. À l'intérieur du panneau de configuration, il y a le gestionnaire de périphériques et là, vous voyez tous vos périphériques donc tous les accessoires qui sont branchés à votre ordinateur, entre autres, la webcam et le micro, et là vous pouvez tout simplement les désactiver.

Animateur : – D'accord.

Steven : – Ça fait que votre ordinateur ne pourra plus les utiliser…

Animateur : – Steven Meyer, CEO et co-fondateur de l'entreprise de cybersécurité Genevoise Zendata, à votre micro Didier Bonvin.

Didier Bonvin : – Oui à noter que les derniers modèles d'écrans de laptop ont désormais une caméra escamotable.

Animateur : – Donc un petit clapet qui permet de la fermer.

Didier : – Voilà exactement.

Animateur : – Vous le faites, vous ? Vous avez maquillé votre…

Didier Bonvin : – Alors, j'ai un bon vieux scotch. Et pour rappel, l'ancien directeur du FBI James Commis, (celui qui a été limogé par Trump) conseillait au grand public de mettre un cache sur les webcams et les micros des ordinateurs. Il y a aussi cette fameuse photo sur Instagram de Marc Zuckerberg, le patron de Facebook, on y voyait son laptop avec un scotch sur la caméra.

Animateur : – Oui voilà, bon peut être que lui il a des raisons d'être hacké mais si lui, oui, alors pourquoi pas nous ? Nous voilà avertis bien protéger son micro et sa webcam chronique de Didier Bourdin écouter sur rts.ch/onenparle sans besoin de nous hacker, on est disponibles et accessibles comme bon vous semble, voilà !