1
00:00:14,466 --> 00:00:17,266
Pour suivre les changements
dans votre environnement de travail,

2
00:00:17,266 --> 00:00:19,266
vous devez apprendre
et évoluer continuellement.

3
00:00:19,566 --> 00:00:23,466
Avec les formations et le coaching
de Cefora, en tant qu'employé(e),

4
00:00:23,466 --> 00:00:26,666
vous affinez vos connaissances
et vos compétences durant votre carrière.

5
00:00:26,833 --> 00:00:28,566
Ainsi, vous continuez
à faire du bon travail.

6
00:00:29,166 --> 00:00:33,133
Lecteur ICT au Collège universitaire
d'Anvers, Dave De Bie allie

7
00:00:33,166 --> 00:00:36,433
sa passion pour la technologie
et la philosophie dans son travail.

8
00:00:36,966 --> 00:00:40,466
En tant que chargé de mission
en IA générative,

9
00:00:40,566 --> 00:00:43,666
il étudie les aspects
éthiques et pratiques de l'IA.

10
00:00:44,033 --> 00:00:48,566
La personne idéale pour un Learning Snack
à propos de Copilot dans Office, donc.

11
00:00:48,933 --> 00:00:51,466
Ces 30 prochaines minutes,
Dave De Bie partagera

12
00:00:51,533 --> 00:00:54,433
sa vision unique et des conseils pratiques

13
00:00:54,466 --> 00:00:57,133
pour donner un coup de fouet
à votre productivité.

14
00:00:57,133 --> 00:01:00,333
Bienvenue au Learning Snack
sur la cybersécurité.

15
00:01:00,466 --> 00:01:05,366
Je m'appelle Dirk Tielens. Aujourd'hui,
je vous donnerai un peu plus de conseils

16
00:01:05,533 --> 00:01:10,033
pour vous sentir plus en sécurité
dans le monde numérique.

17
00:01:10,166 --> 00:01:13,366
Cette présentation
se divisera en trois parties :

18
00:01:13,533 --> 00:01:18,866
tout d'abord, est-il vraiment indispensable
de se protéger dans ce monde numérique,

19
00:01:18,966 --> 00:01:20,566
et pourquoi ?

20
00:01:21,466 --> 00:01:25,066
Dans un deuxième temps,
nous verrons ce qui peut mal tourner.

21
00:01:25,633 --> 00:01:27,833
Que peut-il vous arriver ?

22
00:01:28,166 --> 00:01:32,966
Les ransomwares sont un exemple fréquent,
où vos données se retrouvent cryptées.

23

00:01:33,366 --> 00:01:36,166
Pour terminer,
je vous donnerai quelques astuces

24
00:01:36,333 --> 00:01:40,266
pour mieux vous protéger
contre tous ces risques numériques.

25
00:01:41,433 --> 00:01:44,666
Commençons par comprendre
pourquoi il est si important

26
00:01:45,166 --> 00:01:48,666
d'avoir au moins
une mesure de protection numérique.

27
00:01:49,466 --> 00:01:53,366
Je commencerai par une citation, à savoir :

28
00:01:53,533 --> 00:01:58,466
"Les amateurs piratent les systèmes,
les professionnels piratent les gens."

29
00:01:59,033 --> 00:02:02,566
Cette deuxième approche
est de plus en plus courante de nos jours,

30
00:02:02,733 --> 00:02:05,833
justement parce que les gens,
les utilisateurs finaux,

31
00:02:05,966 --> 00:02:07,866
deviennent le maillon faible.

32
00:02:07,966 --> 00:02:12,166
En effet, les systèmes sont aujourd'hui
bien plus sécurisés qu'avant

33
00:02:12,333 --> 00:02:16,433
et leur piratage devient
de plus en plus compliqué pour les pirates.

34
00:02:16,566 --> 00:02:21,866

Par conséquent,
ils ciblent surtout les utilisateurs,

35
00:02:22,033 --> 00:02:27,466
pour obtenir par exemple leurs identifiants
ou leur double authentification,

36
00:02:27,633 --> 00:02:30,566
ce code requis
pour les opérations bancaires,

37
00:02:30,733 --> 00:02:33,966
en vue d'accéder aux systèmes.

38
00:02:34,366 --> 00:02:36,933
L'époque où des virus

39
00:02:37,066 --> 00:02:41,066
empêchaient le démarrage de votre Windows
est quelque peu révolue.

40
00:02:43,133 --> 00:02:47,166
Autre raison de se protéger : de plus
en plus de données sont dans le cloud.

41
00:02:47,333 --> 00:02:51,066
Avant, les données étaient hébergées
au sein de l'entreprise.

42
00:02:51,166 --> 00:02:54,433
Il fallait y être physiquement
pour accéder aux données.

43
00:02:54,733 --> 00:02:58,566
Désormais, tout est dans le cloud.
Intéressant pour l'utilisateur,

44
00:02:58,733 --> 00:03:01,166
qui peut accéder partout à ses données.

45
00:03:01,366 --> 00:03:04,066
Mais aussi pour le pirate,
qui peut faire de même.

46
00:03:04,466 --> 00:03:07,266
Ajoutons que, consciemment ou non,

47
00:03:07,433 --> 00:03:11,266
on partage plein d'informations
personnelles via les réseaux sociaux,

48
00:03:11,366 --> 00:03:14,366
qui sont évidemment intéressantes
pour les pirates :

49
00:03:14,633 --> 00:03:18,566
dates de naissance de nos enfants
ou noms de nos animaux,

50
00:03:18,733 --> 00:03:22,066
qu'on intègre souvent, consciemment ou non,
à nos mots de passe.

51
00:03:22,166 --> 00:03:26,266
Ce qui facilite les choses aux pirates
pour accéder à ces données.

52
00:03:28,466 --> 00:03:32,466
Les statistiques montrent
que 95 % de tous les cyberincidents

53
00:03:32,633 --> 00:03:34,633
résultent d'erreurs humaines.

54
00:03:34,966 --> 00:03:37,966
De quoi s'agit-il ?
Principalement de phishing,

55
00:03:38,133 --> 00:03:41,866
cet hameçonnage de données
via des SMS ou des mails

56
00:03:42,166 --> 00:03:44,233
invitant à changer un mot de passe.

57

00:03:44,366 --> 00:03:48,966
L'IA jouera d'ailleurs un rôle prépondérant
dans ce domaine à l'avenir, j'y reviendrai.

58
00:03:50,266 --> 00:03:54,933
Des mots de passe faibles sont également
souvent à l'origine de cyberincidents.

59
00:03:55,466 --> 00:03:59,466
Les appareils perdus,
tel le PC portable oublié dans le train.

60
00:04:00,333 --> 00:04:02,833
Ou encore le manque de sensibilisation :

61
00:04:03,233 --> 00:04:07,166
des gens partageant un fichier en externe,

62
00:04:07,266 --> 00:04:09,766
mais l'ouvrant par erreur au monde entier

63
00:04:09,933 --> 00:04:13,333
plutôt qu'aux destinataires prévus.

64
00:04:14,066 --> 00:04:14,966
Et enfin,

65
00:04:15,433 --> 00:04:18,766
l'emploi non sécurisé
de réseaux Wi-Fi publics.

66
00:04:18,933 --> 00:04:21,566
Quand on se connecte
sur un réseau Wi-Fi public,

67
00:04:21,966 --> 00:04:27,533
toutes les données qu'on envoie
peuvent être lues

68
00:04:27,833 --> 00:04:29,833
par quiconque a accès à ce réseau.

69

00:04:29,966 --> 00:04:34,166
Sans autres moyens de protection,
de cryptage complémentaire,

70
00:04:34,533 --> 00:04:39,166
ces données sont directement accessibles,
ce qui n'est évidemment pas souhaité.

71
00:04:41,866 --> 00:04:45,766
Nous avons développé un exemple concret,
qui montre clairement

72
00:04:45,866 --> 00:04:49,566
l'importance de mettre en place
un certain niveau de protection.

73
00:04:49,733 --> 00:04:54,666
Nous avons pour cela utilisé l'exemple
d'un "tenant" de Microsoft 365.

74
00:04:55,066 --> 00:04:59,866
Un "tenant" est l'environnement Microsoft
d'une organisation, ici d'une école.

75
00:05:00,433 --> 00:05:04,766
Cette école compte 2 800 élèves
et près de 600 membres du personnel,

76
00:05:04,933 --> 00:05:07,933
soit presque 3 400 utilisateurs.

77
00:05:08,366 --> 00:05:13,066
Nous avons désactivé
les paramètres de sécurité supplémentaires,

78
00:05:13,233 --> 00:05:16,266
interdisant notamment
les connexions de n'importe où.

79
00:05:16,433 --> 00:05:18,666
On a donc baissé le niveau de protection

80
00:05:18,833 --> 00:05:21,866

et autorisé les connexions de partout.

81
00:05:21,966 --> 00:05:23,866
Voici ce qu'on a constaté

82
00:05:24,366 --> 00:05:28,166
un jour férié, lundi de Pentecôte,
sur une durée de cinq minutes.

83
00:05:28,733 --> 00:05:32,066
Les résultats observés
sont pour le moins inquiétants.

84
00:05:32,166 --> 00:05:37,266
Nous avons constaté quasiment
10 000 tentatives échouées de connexion

85
00:05:37,666 --> 00:05:39,566
sur 41 comptes différents.

86
00:05:39,733 --> 00:05:41,566
Pourquoi 41 spécifiquement ?

87
00:05:41,833 --> 00:05:45,266
Il s'agit de comptes
dont l'adresse e-mail est connue.

88
00:05:45,366 --> 00:05:49,333
Les pirates ont tout simplement essayé
de se connecter à ces comptes.

89
00:05:49,466 --> 00:05:52,766
Soyons clairs :
ils n'ont accédé à aucun de ces comptes,

90
00:05:52,933 --> 00:05:54,666
mais ils s'y sont essayés.

91
00:05:55,266 --> 00:05:58,733
Au cours de ces cinq minutes,
un compte en particulier

92

00:05:58,866 --> 00:06:02,066
a enregistré 1 220 tentatives de connexion.

93
00:06:03,866 --> 00:06:06,633
Et sur ces 41 comptes, il y en avait six

94
00:06:06,766 --> 00:06:11,833
ayant enregistré plus de 1 000 tentatives
de connexion en cinq minutes.

95
00:06:12,366 --> 00:06:15,733
Il s'agissait d'ailleurs
de comptes de membres du personnel,

96
00:06:15,866 --> 00:06:17,633
dont un membre de la direction.

97
00:06:18,866 --> 00:06:24,066
Les attaques provenaient d'un peu partout,
de 108 pays pour être exact,

98
00:06:24,233 --> 00:06:27,066
mais principalement de Chine,
de Corée du Sud,

99
00:06:27,733 --> 00:06:33,233
des États-Unis, de Hong Kong
et des Émirats Arabes Unis.

100
00:06:35,366 --> 00:06:38,466
Maintenant,
lorsqu'on est victimes d'une attaque,

101
00:06:38,633 --> 00:06:42,166
que peut-il nous arriver ?
Qu'est-ce qui peut mal tourner ?

102
00:06:42,666 --> 00:06:46,266
Eh bien, la conséquence
la plus courante de nos jours

103
00:06:46,433 --> 00:06:50,133
est la perte de données,

principalement par le biais du ransomware.

104
00:06:50,266 --> 00:06:52,366
Un ransomware est un logiciel,

105
00:06:52,466 --> 00:06:58,166
récupéré en installant un package logiciel
issu d'un site malveillant,

106
00:06:58,666 --> 00:07:00,833
qui va crypter vos données.

107
00:07:00,966 --> 00:07:03,566
C'est-à-dire que vos fichiers personnels,

108
00:07:03,733 --> 00:07:07,566
photos, documents et autres,
deviennent inutilisables.

109
00:07:07,766 --> 00:07:13,566
Ils sont pour ainsi dire verrouillés
dans un coffre-fort par le pirate.

110
00:07:13,966 --> 00:07:18,266
Et sans la clé logicielle,
on ne peut plus rien en faire.

111
00:07:18,466 --> 00:07:21,766
Les victimes les plus connues
d'une attaque de ransomware

112
00:07:21,866 --> 00:07:26,766
sont les villes d'Anvers,
de Diest et de Zwijndrecht.

113
00:07:27,233 --> 00:07:32,433
La marque Duvel, il y a peu,
ainsi que bien d'autres, évidemment.

114
00:07:32,733 --> 00:07:35,666
Mais si on en est la victime
et si on n'a pas de back-up,

115
00:07:36,066 --> 00:07:38,466
on se trouve devant un sérieux problème.

116
00:07:40,466 --> 00:07:45,366
Veeam, une société renommée
développant des logiciels de back-up,

117
00:07:45,533 --> 00:07:47,166
a même organisé un sondage

118
00:07:47,333 --> 00:07:51,333
auprès de 12 000 utilisateurs
ayant été victimes d'une cyberattaque.

119
00:07:51,666 --> 00:07:52,933
Ce sondage montre

120
00:07:53,366 --> 00:07:57,966
que 41 % des données est touché,

121
00:07:58,766 --> 00:08:04,133
dont seul 57 % peut être récupéré.

122
00:08:04,933 --> 00:08:09,766
Donc en cas d'attaque,
41 % des données en moyenne sera crypté

123
00:08:10,166 --> 00:08:12,066
et sur ces données cryptées,

124
00:08:12,733 --> 00:08:17,466
un peu moins de deux tiers seulement
peut être récupéré.

125
00:08:17,633 --> 00:08:19,533
Voilà des chiffres hallucinants

126
00:08:19,966 --> 00:08:22,766
qui peuvent vous faire réfléchir.

127
00:08:23,866 --> 00:08:26,966

Et quelques chiffres
qui m'ont moi-même effrayé :

128
00:08:27,066 --> 00:08:31,466
quatre victimes sur cinq paient
pour récupérer leurs données.

129
00:08:31,633 --> 00:08:36,166
Il n'y a pourtant aucune garantie
de récupérer les données en payant,

130
00:08:36,333 --> 00:08:40,666
comme on le voit plus bas : une victime
sur trois n'a pas pu récupérer ses données.

131
00:08:41,033 --> 00:08:46,133
Mais étrangement, la plupart des sociétés,
sans doute pour des raisons économiques,

132
00:08:46,366 --> 00:08:51,366
semblent payer lorsqu'elles sont victimes
d'une attaque de ransomware.

133
00:08:54,833 --> 00:08:56,466
Que peut-il arriver d'autre ?

134
00:08:56,633 --> 00:09:00,133
Que quelqu'un obtienne accès à vos données

135
00:09:00,266 --> 00:09:02,533
ou que celles-ci soient disséminées.

136
00:09:02,666 --> 00:09:05,433
Outre la perte de données
dont on vient de parler,

137
00:09:05,866 --> 00:09:10,666
nos données peuvent atterrir sur Internet
alors qu'on voudrait l'éviter.

138
00:09:10,833 --> 00:09:14,366
Ça arrive très souvent via le phishing :
pensez notamment

139
00:09:14,466 --> 00:09:17,666
aux pirates mettant la main
sur vos données bancaires.

140
00:09:17,933 --> 00:09:22,000
L'IA va jouer un rôle important
dans ce domaine. On connaît tous les SMS

141
00:09:22,133 --> 00:09:26,933
du fils ou de la fille vous demandant
de lui faire un virement urgent.

142
00:09:28,033 --> 00:09:32,333
Eh bien, à l'avenir, vous recevrez
carrément un appel de votre enfant.

143
00:09:32,500 --> 00:09:36,433
C'est-à-dire
qu'avec la voix de votre fille ou fils,

144
00:09:36,600 --> 00:09:40,500
trouvée sur Internet,
ils monteront un autre message

145
00:09:40,633 --> 00:09:44,233
et ainsi tenter de vous faire croire

146
00:09:44,333 --> 00:09:46,533
que vous parlez à votre enfant

147
00:09:46,700 --> 00:09:50,300
et de vous faire transmettre
les codes dont ils ont besoin.

148
00:09:50,933 --> 00:09:55,533
Les vidéos deepfakes joueront aussi
un grand rôle dans l'hameçonnage à l'avenir.

149
00:09:55,700 --> 00:09:58,300
Autre nouveauté : les malwares polymorphes.

150

00:09:58,433 --> 00:10:00,933
Un malware est un logiciel malveillant.

151
00:10:01,333 --> 00:10:05,533
Et un malware polymorphe
est un malware qui se réécrit lui-même

152
00:10:05,700 --> 00:10:10,533
afin de mieux échapper à la détection
par les logiciels antivirus.

153
00:10:12,933 --> 00:10:15,133
Une troisième conséquence possible,

154
00:10:15,300 --> 00:10:19,433
outre la perte de données
et l'accès aux données,

155
00:10:19,900 --> 00:10:21,900
est la paralysie des systèmes,

156
00:10:22,800 --> 00:10:25,600
notamment via ce qu'on appelle
des attaques DDoS.

157
00:10:25,733 --> 00:10:29,933
Il s'agit d'attaques
ciblant très spécifiquement le système

158
00:10:30,100 --> 00:10:32,133
plutôt que les utilisateurs finaux.

159
00:10:32,300 --> 00:10:37,133
Par ce biais, ils peuvent par exemple
couper votre connexion Internet.

160
00:10:37,500 --> 00:10:40,300
En un mot, une attaque DDoS

161
00:10:40,433 --> 00:10:43,533
transmet une telle quantité de données
à un système

162
00:10:43,633 --> 00:10:45,600
que ce dernier devient inutilisable.

163
00:10:45,733 --> 00:10:48,633
Vous remarquerez
que votre connexion Internet

164
00:10:49,633 --> 00:10:50,733
se retrouve coupée.

165
00:10:51,400 --> 00:10:54,033
De plus, ces attaques
sont très simples à lancer.

166
00:10:54,200 --> 00:10:57,000
J'y ai moi-même été confronté
à plusieurs reprises

167
00:10:57,133 --> 00:10:59,433
et le plus jeune coupable avait onze ans.

168
00:10:59,533 --> 00:11:01,800
C'était un élève de 6e.

169
00:11:02,200 --> 00:11:05,233
Les écoles
y sont particulièrement confrontées,

170
00:11:05,333 --> 00:11:10,233
puisque les élèves peuvent ainsi paralyser
temporairement l'Internet de l'école.

171
00:11:10,800 --> 00:11:12,400
On peut s'en prémunir,

172
00:11:12,533 --> 00:11:17,733
mais cela s'accompagne
d'un coût plutôt élevé.

173
00:11:18,233 --> 00:11:22,633
Mais il s'agit d'une situation
très problématique quand on s'y trouve.

174
00:11:23,400 --> 00:11:26,300
Voici un exemple concret d'une attaque DDoS.

175
00:11:26,433 --> 00:11:29,633
Nous avons ici le monitoring
d'une connexion Internet.

176
00:11:29,733 --> 00:11:32,500
Le graphique en deuxième ligne

177
00:11:32,633 --> 00:11:35,433
montre une ligne verte et une ligne bleue.

178
00:11:35,533 --> 00:11:39,200
La ligne verte en haut montre
si la connexion Internet est active.

179
00:11:39,333 --> 00:11:43,500
La ligne bleue indique le temps de réponse,
actuellement d'environ 20 ms.

180
00:11:43,633 --> 00:11:45,733
En bas, on voit que la ligne est active.

181
00:11:46,133 --> 00:11:47,733
Lorsqu'une attaque a lieu,

182
00:11:47,833 --> 00:11:51,133
comme celle que je lance
via le site que j'ai ouvert à droite,

183
00:11:51,233 --> 00:11:55,000
on voit que la connexion Internet

184
00:11:55,133 --> 00:11:58,733
chute rapidement
et se retrouve inaccessible.

185
00:11:58,900 --> 00:12:01,833
On le constate dans le graphique
comme le tableau.

186
00:12:02,000 --> 00:12:05,700
Le tableau en bas répète clairement
"No internet connection".

187
00:12:05,833 --> 00:12:09,900
Actuellement,
un certain nombre de PC sont en train,

188
00:12:10,200 --> 00:12:13,333
tels des bots,
d'envoyer de telles quantités de données

189
00:12:13,500 --> 00:12:17,200
à cette connexion Internet
que celle-ci devient injoignable,

190
00:12:17,333 --> 00:12:20,833
en l'occurrence
pendant une trentaine de secondes.

191
00:12:20,933 --> 00:12:23,633
On voit que la connexion
commence à se rétablir,

192
00:12:23,733 --> 00:12:25,833
dans le tableau comme le graphique.

193
00:12:26,100 --> 00:12:29,033
Sa stabilisation complète
prendra un petit moment.

194
00:12:29,300 --> 00:12:34,400
Comme vous le voyez,
le site que j'ai ouvert à droite,

195
00:12:34,533 --> 00:12:39,333
est un simple site sur lequel il suffit
d'entrer quelques informations

196
00:12:39,433 --> 00:12:44,733
puis de cliquer sur "Envoyer attaque"
pour paralyser une connexion Internet.

197
00:12:46,733 --> 00:12:49,300
Dernier paramètre, qu'on oublie souvent :

198
00:12:49,433 --> 00:12:51,733
les risques venant de l'intérieur.

199
00:12:52,833 --> 00:12:58,000
Un employé rancunier, par exemple,
peut également représenter une menace.

200
00:12:58,533 --> 00:13:01,233
Un employé mécontent d'être renvoyé

201
00:13:01,333 --> 00:13:06,100
qui déciderait de laisser sa carte de visite

202
00:13:06,733 --> 00:13:08,933
peut provoquer pas mal d'embêtements.

203
00:13:09,033 --> 00:13:14,500
Ainsi, un compte non clôturé après
le licenciement ou le départ d'un employé...

204
00:13:14,633 --> 00:13:17,900
J'observe bien souvent
dans des organisations

205
00:13:18,033 --> 00:13:22,833
que des personnes inactives depuis des mois
ont toujours accès à leur compte.

206
00:13:23,600 --> 00:13:27,733
On l'a évoqué, un collaborateur
peut partager publiquement ses données

207
00:13:27,900 --> 00:13:31,333
donc avec le monde entier
plutôt que des personnes spécifiques.

208
00:13:32,033 --> 00:13:36,333
Un conseil utile à ce sujet : évitez

les comptes et les mots de passe partagés.

209
00:13:36,500 --> 00:13:40,433
On voit bien trop souvent des comptes
utilisés par plusieurs personnes.

210
00:13:40,600 --> 00:13:43,733
On ne maîtrise alors pas du tout
qui possède ces données,

211
00:13:43,900 --> 00:13:48,200
qui seront aisément transmises.
Prenez un mot de passe Wi-Fi :

212
00:13:49,400 --> 00:13:51,100
si une ou deux personnes l'ont,

213
00:13:51,233 --> 00:13:54,933
c'est une question de temps
avant que toute l'organisation

214
00:13:55,300 --> 00:13:59,300
et même des personnes non autorisées
ne récupèrent ce mot de passe.

215
00:14:01,200 --> 00:14:05,000
Voilà les problèmes qu'on peut rencontrer.
Comment s'en prémunir ?

216
00:14:05,133 --> 00:14:07,933
Il va de soi que l'IT lui-même
joue un grand rôle

217
00:14:08,100 --> 00:14:10,333
et bloque une bonne partie des risques,

218
00:14:10,433 --> 00:14:13,733
mais l'utilisateur final
peut aussi se protéger

219
00:14:14,100 --> 00:14:16,133
contre un certain nombre de risques.

220
00:14:16,700 --> 00:14:19,333
Le moyen le plus important et le plus connu

221
00:14:19,433 --> 00:14:22,233
est bien sûr
l'authentification multifacteur.

222
00:14:22,400 --> 00:14:25,533
L'authentification multifacteur,
c'est simplement

223
00:14:25,833 --> 00:14:29,833
le fait de s'identifier
de plusieurs manières différentes,

224
00:14:29,933 --> 00:14:34,033
de prouver son identité par plus d'un biais.

225
00:14:34,333 --> 00:14:37,933
Les plus connus sont
les authentifications Microsoft et Google.

226
00:14:38,100 --> 00:14:43,200
Il s'agit d'une sorte de code à demander
depuis votre GSM lors d'une connexion,

227
00:14:43,633 --> 00:14:48,633
qui vient prouver que vous avez le GSM
de l'utilisateur en mains,

228
00:14:48,733 --> 00:14:52,700
car ce code ne peut être demandé
que depuis un GSM donné.

229
00:14:52,833 --> 00:14:57,433
Plus compliqué, donc, pour les pirates,
car même s'ils ont votre mot de passe,

230
00:14:57,733 --> 00:15:00,033
il leur faut encore le code de votre GSM.

231
00:15:00,200 --> 00:15:03,333

Sans votre GSM,
ils ne devraient donc pas pouvoir entrer.

232
00:15:03,833 --> 00:15:06,700
Parfois, le code peut aussi
nous parvenir par SMS.

233
00:15:07,533 --> 00:15:09,300
Et un autre moyen très pratique

234
00:15:10,700 --> 00:15:16,033
combinant confort d'utilisation et sécurité
mais un peu moins connu aujourd'hui,

235
00:15:16,300 --> 00:15:18,100
est Windows Hello for Business.

236
00:15:18,233 --> 00:15:21,533
Je vous montre en capture d'écran
comment le programmer :

237
00:15:21,700 --> 00:15:25,733
c'est très simple pour l'utilisateur final,
même si l'IT doit l'activer.

238
00:15:26,033 --> 00:15:32,400
Il vous permettra de vous connecter
à votre PC via un simple code PIN

239
00:15:32,533 --> 00:15:36,800
tout en étant protégé
par une authentification multifacteur.

240
00:15:36,933 --> 00:15:42,733
La deuxième preuve de votre identité,
en effet,

241
00:15:42,900 --> 00:15:45,333
est votre appareil lui-même.

242
00:15:45,633 --> 00:15:47,533
Ainsi, l'appareil et le code PIN,

243
00:15:47,633 --> 00:15:51,800
qui ne fonctionnera que sur cet appareil-là,
prouvent votre identité.

244
00:15:51,933 --> 00:15:54,233
Deux preuves : le code PIN et l'appareil.

245
00:15:54,400 --> 00:15:58,900
C'est similaire à votre carte bancaire,
où vous avez le code PIN et la carte.

246
00:16:00,600 --> 00:16:03,833
Je vous montre à quoi ressemble
Windows Hello for Business.

247
00:16:04,000 --> 00:16:07,333
On peut ici s'identifier
via le code PIN ou un mot de passe.

248
00:16:07,433 --> 00:16:10,533
En bas,
les deux boutons permettent de choisir

249
00:16:10,733 --> 00:16:12,333
le code PIN ou le mot de passe.

250
00:16:12,433 --> 00:16:15,233
Une fois Windows Hello for Business activé,

251
00:16:15,333 --> 00:16:19,833
vous n'avez qu'à entrer les quatre chiffres
de votre code PIN pour vous connecter.

252
00:16:20,233 --> 00:16:25,000
Une deuxième méthode pour vous protéger
est un bon gestionnaire de mots de passe.

253
00:16:25,433 --> 00:16:29,833
C'est un genre de coffre-fort numérique
stockant tous vos mots de passe.

254
00:16:30,100 --> 00:16:32,700

Vous n'aurez donc
plus qu'un seul mot de passe.

255
00:16:32,833 --> 00:16:36,133
Qu'il ne faudra pas oublier,
sans quoi vous aurez un souci.

256
00:16:36,800 --> 00:16:39,233
Un tel outil vous permet donc

257
00:16:39,400 --> 00:16:44,533
d'accéder à un site en saisissant
automatiquement votre mot de passe.

258
00:16:44,700 --> 00:16:50,533
De nos jours, les navigateurs ont ça aussi,
mais leurs possibilités sont plus limitées.

259
00:16:51,400 --> 00:16:54,900
Il existe quelques bons gestionnaires
de mots de passe,

260
00:16:55,033 --> 00:16:58,300
tels LastPass, 1Password,
Bitwarden ou Keepass.

261
00:16:58,800 --> 00:17:00,500
Ce sont tous de bons exemples.

262
00:17:00,833 --> 00:17:06,400
L'un sera plus efficace que l'autre,
selon ses fonctionnalités

263
00:17:06,533 --> 00:17:11,033
et les critiques
qu'il aura récemment reçues dans les médias.

264
00:17:11,833 --> 00:17:13,433
Une astuce complémentaire :

265
00:17:13,600 --> 00:17:17,633
utilisez pour chaque site un mot de passe
unique suffisamment complexe.

266
00:17:17,733 --> 00:17:20,933
Si vous faites ça, pas besoin
de gestionnaire de mots de passe,

267
00:17:21,100 --> 00:17:26,933
mais il est compliqué d'apprendre par cœur
tous ces mots de passe.

268
00:17:27,833 --> 00:17:30,800
LastPass est
un de ces gestionnaires de mots de passe.

269
00:17:30,933 --> 00:17:32,800
Vous voyez ici la sauvegarde

270
00:17:32,933 --> 00:17:36,033
de plusieurs identifiants
et notes dans LastPass.

271
00:17:36,133 --> 00:17:39,600
On peut aussi y déposer des notes,
comme le code de votre alarme

272
00:17:40,000 --> 00:17:42,633
ou les codes PIN ou PUK de vos GSM.

273
00:17:42,800 --> 00:17:46,733
En fait, on peut y saisir
toutes sortes d'informations.

274
00:17:47,200 --> 00:17:52,633
On y a ainsi déposé
un identifiant pour Outlook Live.

275
00:17:52,733 --> 00:17:55,633
Et ce qui est pratique,
c'est que pour ouvrir le site,

276
00:17:55,933 --> 00:17:59,533
plus besoin de s'y rendre manuellement
et d'y saisir ses données.

277
00:17:59,700 --> 00:18:02,533
On clique simplement sur le site
dans LastPass,

278
00:18:03,000 --> 00:18:06,333
et LastPass y saisira automatiquement
vos données.

279
00:18:06,433 --> 00:18:09,933
Vous arrivez sur le site,
vous connectez automatiquement

280
00:18:10,033 --> 00:18:12,533
et, sans avoir saisi
le moindre mot de passe,

281
00:18:13,033 --> 00:18:15,233
entrez dans le système.

282
00:18:15,333 --> 00:18:17,933
C'est très pratique.

283
00:18:18,633 --> 00:18:23,300
En outre, il est aussi très intéressant
d'ajouter des comptes à LastPass.

284
00:18:23,433 --> 00:18:26,600
Imaginons que vous créez un compte
sur un site Internet.

285
00:18:26,833 --> 00:18:30,533
Vous devrez bien sûr saisir
votre e-mail et votre mot de passe,

286
00:18:30,633 --> 00:18:34,833
mais une fois que vous aurez saisi
toutes ces informations,

287
00:18:35,633 --> 00:18:39,233
LastPass le détectera et vous proposera

288
00:18:39,333 --> 00:18:44,233

de sauvegarder dans son coffre-fort
le mot de passe que vous avez saisi

289
00:18:44,333 --> 00:18:49,100
pour une consultation ultérieure simplifiée.
C'est la notification en haut à droite.

290
00:18:49,233 --> 00:18:52,400
Je peux aussi choisir
le dossier d'enregistrement

291
00:18:52,533 --> 00:18:54,933
et sélectionner certaines options.

292
00:18:55,233 --> 00:19:00,033
Dès que je clique sur "Ajouter",
ce compte est ajouté au coffre-fort.

293
00:19:00,133 --> 00:19:04,300
En cliquant sur l'add-on du navigateur,
on observe qu'il a été ajouté.

294
00:19:04,433 --> 00:19:09,933
Et sur LastPass même,
on verra que ces données y apparaissent.

295
00:19:10,033 --> 00:19:14,833
Je rafraîchis la page
et on voit apparaître les données.

296
00:19:15,000 --> 00:19:17,800
On peut alors accéder d'ici au site coolblue

297
00:19:17,933 --> 00:19:23,733
ou en afficher les données
et se connecter au site par ce biais.

298
00:19:24,733 --> 00:19:27,233
Nous en avons bientôt terminé.

299
00:19:27,400 --> 00:19:30,500
Un conseil que j'aimerais encore donner

300
00:19:30,633 --> 00:19:32,733
est d'utiliser votre bon sens.

301
00:19:33,133 --> 00:19:36,300
On ne le dit pas assez, mais bien souvent,

302
00:19:36,433 --> 00:19:39,600
le SMS ou l'e-mail donne des indices
permettant de voir

303
00:19:39,733 --> 00:19:44,733
si on cherche à vous soutirer des données,
s'il s'agit d'un mail d'hameçonnage.

304
00:19:45,133 --> 00:19:49,800
Il y a un test pour tester vos connaissances
sur safeonweb.be,

305
00:19:49,933 --> 00:19:51,333
un site gouvernemental

306
00:19:51,633 --> 00:19:54,933
vous permettant d'estimer
au moyen d'exemples concrets

307
00:19:55,333 --> 00:19:58,633
si vous savez ou non
démasquer un mail d'hameçonnage.

308
00:19:58,800 --> 00:20:00,800
Et une règle à garder en tête :

309
00:20:01,133 --> 00:20:06,333
si ça semble trop beau pour être vrai,
c'est généralement le cas.

310
00:20:08,733 --> 00:20:12,633
Et bien sûr, même si ça s'applique moins
à l'utilisateur final,

311
00:20:13,333 --> 00:20:18,200
l'IT peut également apporter son aide.

Il existe des outils à cet effet :

312
00:20:18,533 --> 00:20:22,733
faites aussi souvent que possible
des mises à jour sur votre appareil.

313
00:20:22,833 --> 00:20:25,400
Bien des mises à jour concernent la sécurité

314
00:20:25,533 --> 00:20:28,433
et viennent consolider
les points vulnérables.

315
00:20:29,300 --> 00:20:32,700
Ne négligez donc pas les mises à jour
pendant des années.

316
00:20:33,133 --> 00:20:36,933
Antivirus et pare-feu sont indispensables
de nos jours sur votre PC

317
00:20:37,333 --> 00:20:41,633
et peuvent éventuellement aussi
apporter une valeur ajoutée sur votre GSM.

318
00:20:42,733 --> 00:20:47,633
Sans eux, vous serez
bien plus vulnérables à tous ces risques.

319
00:20:49,233 --> 00:20:51,233
Pour finir, une astuce sympa :

320
00:20:51,633 --> 00:20:55,033
vous pouvez vous-même vérifier
si votre e-mail ou mot de passe

321
00:20:55,133 --> 00:20:58,200
circulent sur Internet
dans le circuit illégal

322
00:20:58,333 --> 00:21:00,800
ou se trouvent dans une base de données

323
00:21:00,933 --> 00:21:03,800
ayant déjà été proposée à la vente
sur le Dark Web.

324
00:21:04,300 --> 00:21:07,933
Ce site s'appelle haveibeenpwned.com.

325
00:21:08,033 --> 00:21:09,433
Vous pouvez vous y rendre

326
00:21:09,833 --> 00:21:15,100
et y saisir votre adresse e-mail
ou mot de passe pour vérifier

327
00:21:15,233 --> 00:21:19,733
si vos données se trouvent
dans une base de données ayant fuité.

328
00:21:19,833 --> 00:21:23,733
Si oui, changez vite votre mot de passe
pour être de nouveau protégés.

329
00:21:24,033 --> 00:21:28,233
On peut aussi y observer
que le mot de passe "123456"

330
00:21:28,400 --> 00:21:31,233
est employé quelque 42 millions de fois
ou, du moins,

331
00:21:31,400 --> 00:21:34,733
est référencé 42 millions de fois
dans cette base de données.

332
00:21:34,833 --> 00:21:37,733
Il peut donc être intéressant de voir
ce qu'il en est

333
00:21:37,900 --> 00:21:40,333
pour vos données personnelles.

334
00:21:40,500 --> 00:21:42,900

Voilà pour ces quelques astuces concrètes

335
00:21:43,033 --> 00:21:46,533
que je voulais vous prodiguer
autour de la cybersécurité.