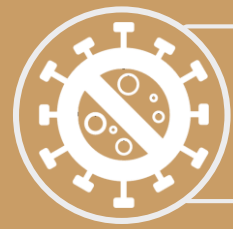
rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

Cyber sécurité et COVID 19

Un guide pratique pour les institutions financières (IF)

03/12/2020



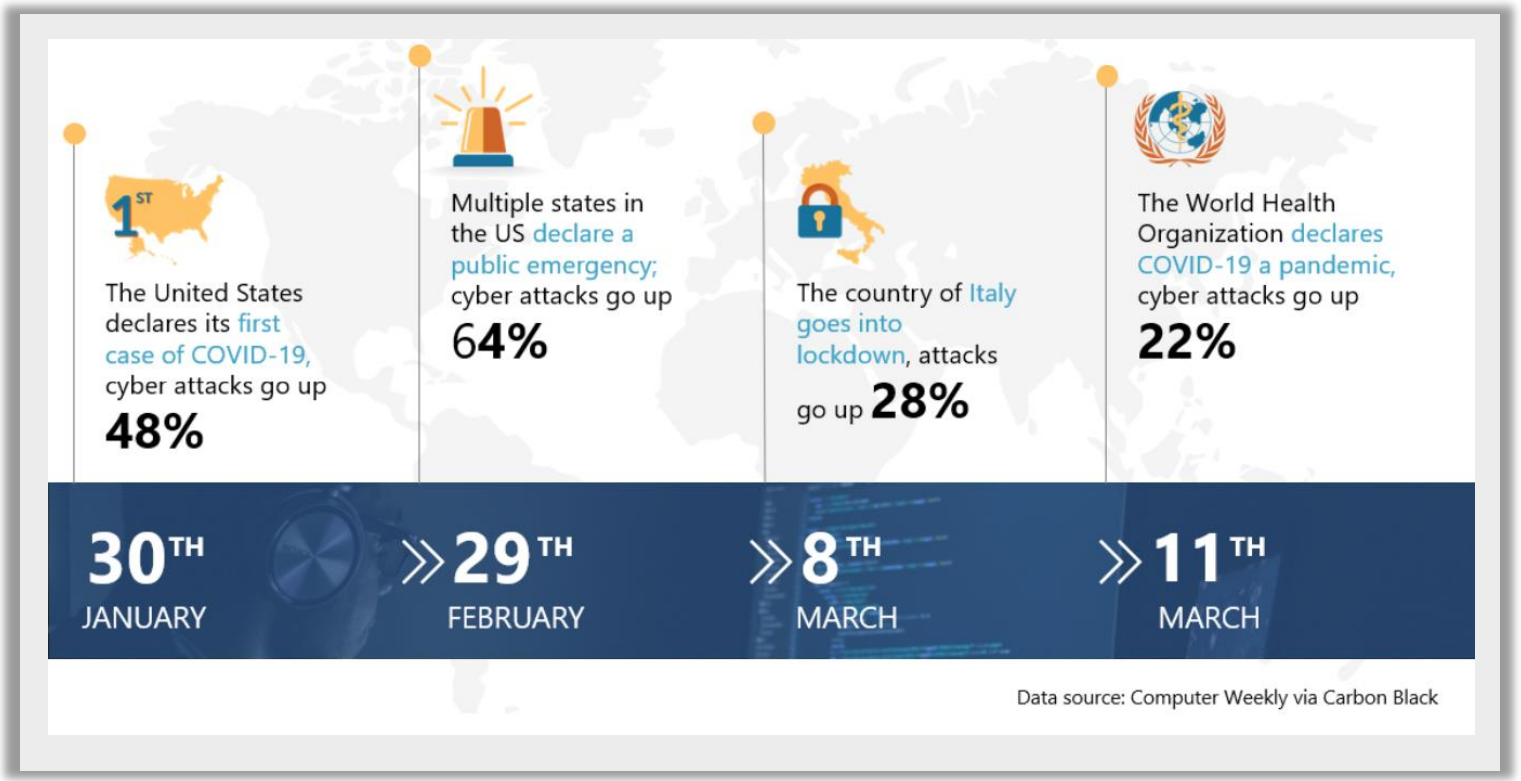
FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!

rsbp Programme régional PME Tunisie

Table des matières

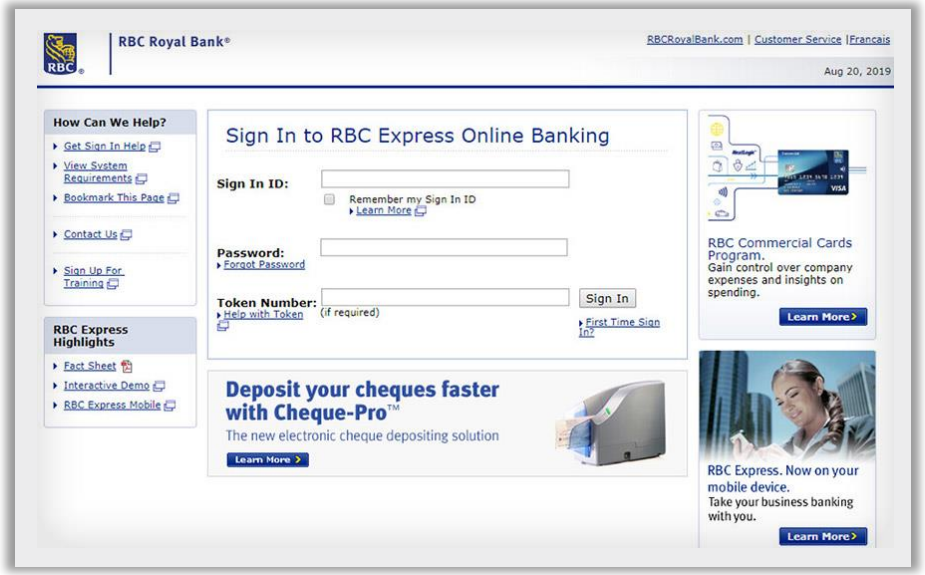
Banque Européenne pour la Reconstruction et le Développement

Cyber sécurité défis



- Une numérisation accélérée
- Besoin de nouveaux canaux
- Travail à distance
- Augmentation des attaques
  - 52 % des cyber-attaques des IF en mars 2020 (Source : VMware)
  - Augmentation de 38 % des cyber-attaques des IF (Source : Computer Weekly)

Situation



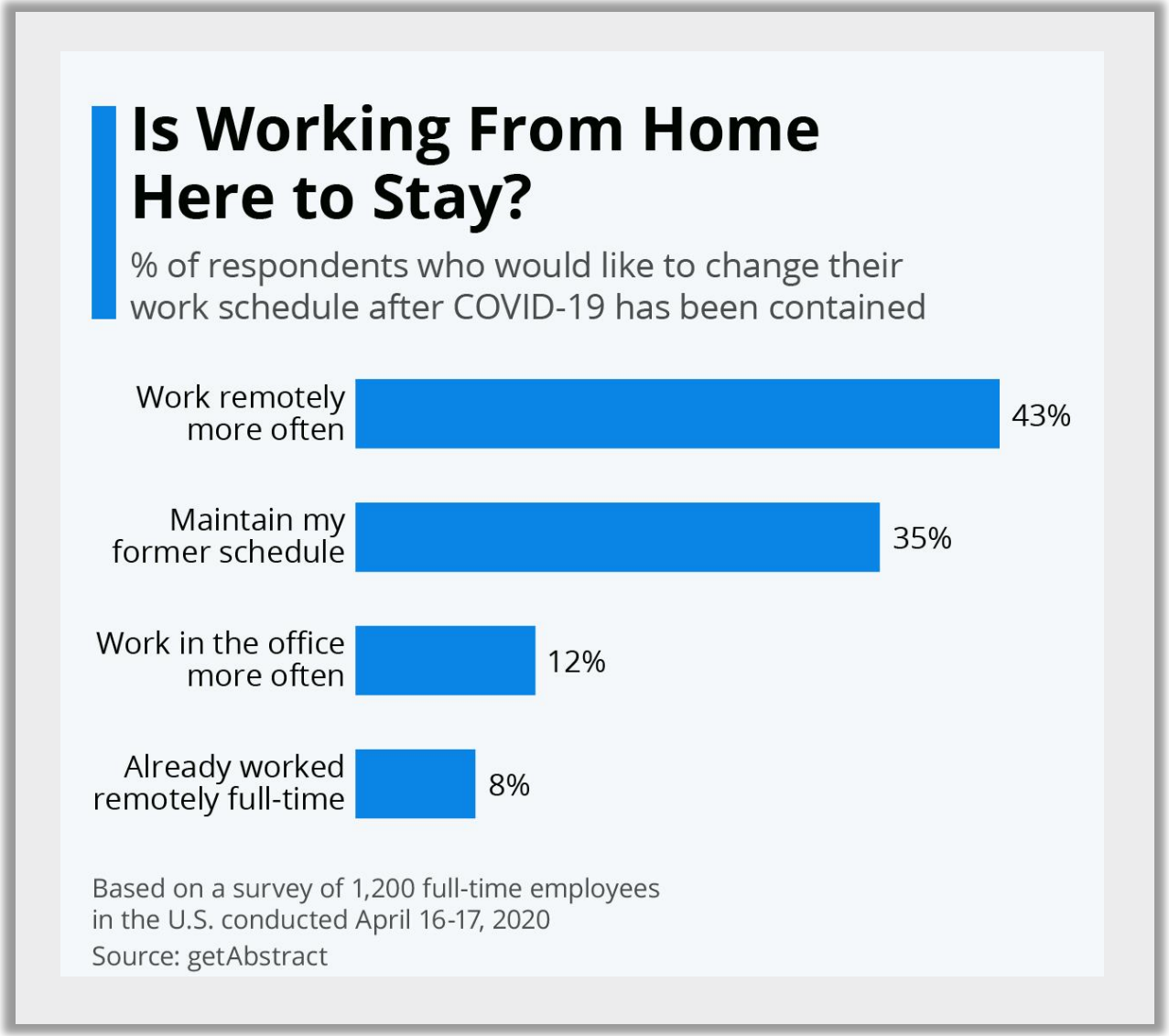
- ❑ Scripts intersites (XSS)
- ❑ Phishing
- ❑ DDOS
- ❑ Ransomware

Principales menaces

Travail à distance

Situation

- ❑ Mise en œuvre rapide
- ❑ Infrastructures non adaptées
- ❑ Manque d'information des employés
- ❑ Des mesures de sécurité insuffisantes
- ❑ La nouvelle norme ?
- ❑ Politiques à réviser



Accès à distance aux logiciels

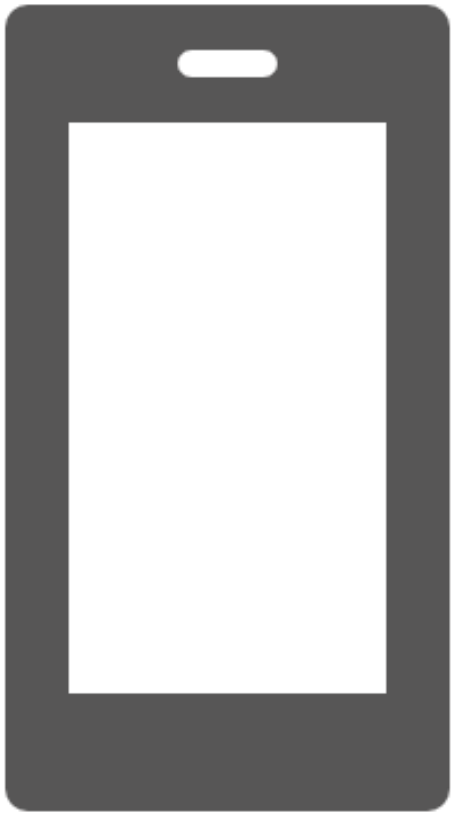
- ✓ Authentification multi-facteurs
- ✓ Politique en matière de mots de passe
- ✓ VPN contre RDP
- ✓ Ordinateurs privés
  - ✓ Sécuriser le Wifi à domicile
  - ✓ Antivirus

Réunions virtuelles

- ✓ Protection de l'accès
  - ✓ Mot de passe
  - ✓ Lobby
- ✓ Partage sécurisé
- ✓ Enregistrement

Prévention des pertes de données

- ✓ Garder le professionnel loin du personnel
- ✓ Utilisation de périphériques externes
- ✓ Sauvegardes régulières

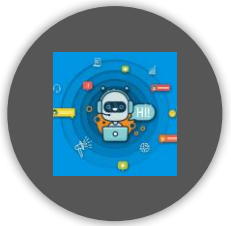


Canaux numériques

Nouveaux canaux, nouveaux risques

BANQUE MOBILE

BANQUE PAR INTERNET



CHAT BOTS

Centre de données

- Serveurs web
- Base de données

Dispositif

- Phishing
- Téléchargement

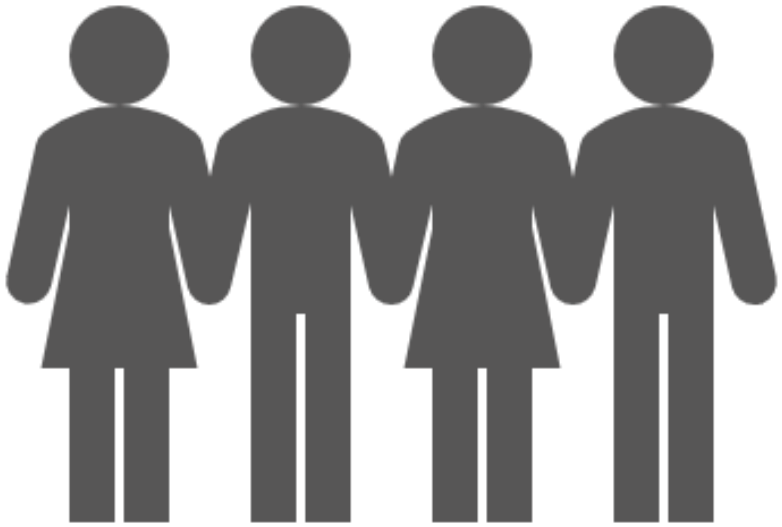
Réseau

- Le wi-fi non sécurisé
- Échange de données non cryptées

Sécuriser les canaux numériques

- ✓ Limites d'authentification
- ✓ Authentification biométrique
- ✓ Communication cryptée
- ✓ Autodestruction
- ✓ Paramétrage sécurisé
- ✓ Mises à jour régulières
- ✓ Lignes directrices pour la sécurisation des applications mobiles

https://owasp.org/www-project-mobile-security/



Réponse institutionnelle

Réponse de l'institution

- ✓ Identification et classification des biens informatiques
- ✓ Identification des fonctions essentielles
- ✓ Évaluations de la vulnérabilité et tests de pénétration
- ✓ Authentification multi-facteurs pour l'accès externe
- ✓ Chiffrement des données stockées sur les appareils portables
- ✓ Surveillance, détection et réaction continues
- ✓ Planification et préparation de la réponse aux incidents cybernétiques
- ✓ Maintenir une bonne cyberhygiène
- ✓ Plans de communication de crise

Mesures pratiques

- ✓ Sécurité du courrier électronique
- ✓ Protection par mot de passe
- ✓ Sécurité sur le web
- ✓ Maintenance des appareils
- ✓ Distribution de l'information