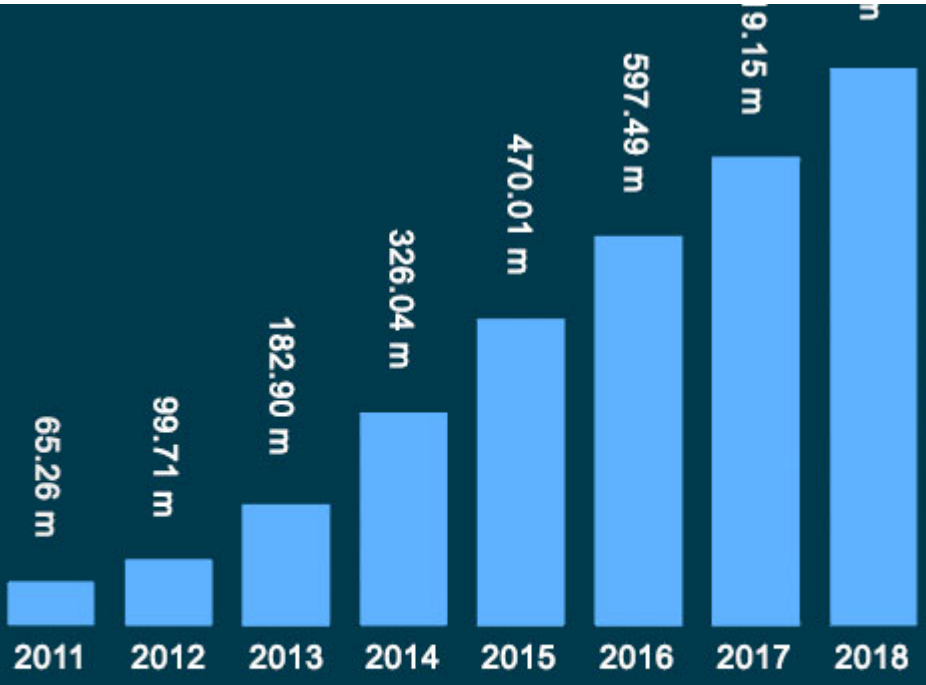
Bring your Own Device Policies

Not having a Bring Your Own Device policy puts your organization at risk for viruses and hacker attacks. Every year the number of attacks goes up, and the need to protect your data and devices becomes more critical.
MALWARE STATS BY YEAR:
856.62 m



Malware samples have been increasing steadily since 2010, every year organizations are at greater and greater risk.

Source: https://www.av-test.org/en/statistics/malware/

MALWARE FACTS:

MOST EXPENSIVE

The most expensive computer virus ever **"MyDoom"** caused $38.5 billion in total damages between 2002 and 2004.

INCREASING RISK

It is estimated that by 2022, there will be over 6 billion internet users. That is a lot of potential victims!

THE ODDS OF YOUR IDENTITY BEING stolen in the next year is about 1 in 20. Every year over 9 million Americans have their identities stolen.

TYPES OF CYBER ATTACKS:

Source: www.breachlevelindex.com

69% IDENTITY THEFT

FINANCIAL ACCESS 16%

7% ACCOUNT ACCESS

5% DATA ACCESS

3% NUISANCE

64%
OF ORGANIZATIONS HAVE A WRITTEN BYOD POLICY
81%
OF ORGANIZATIONS REQUIRE A SIGNED POLICY
36%
OF ORGANIZATIONS REQUIRE SIGNING A CONTRACT

SO WHAT ARE ORGANIZATIONS DOING?

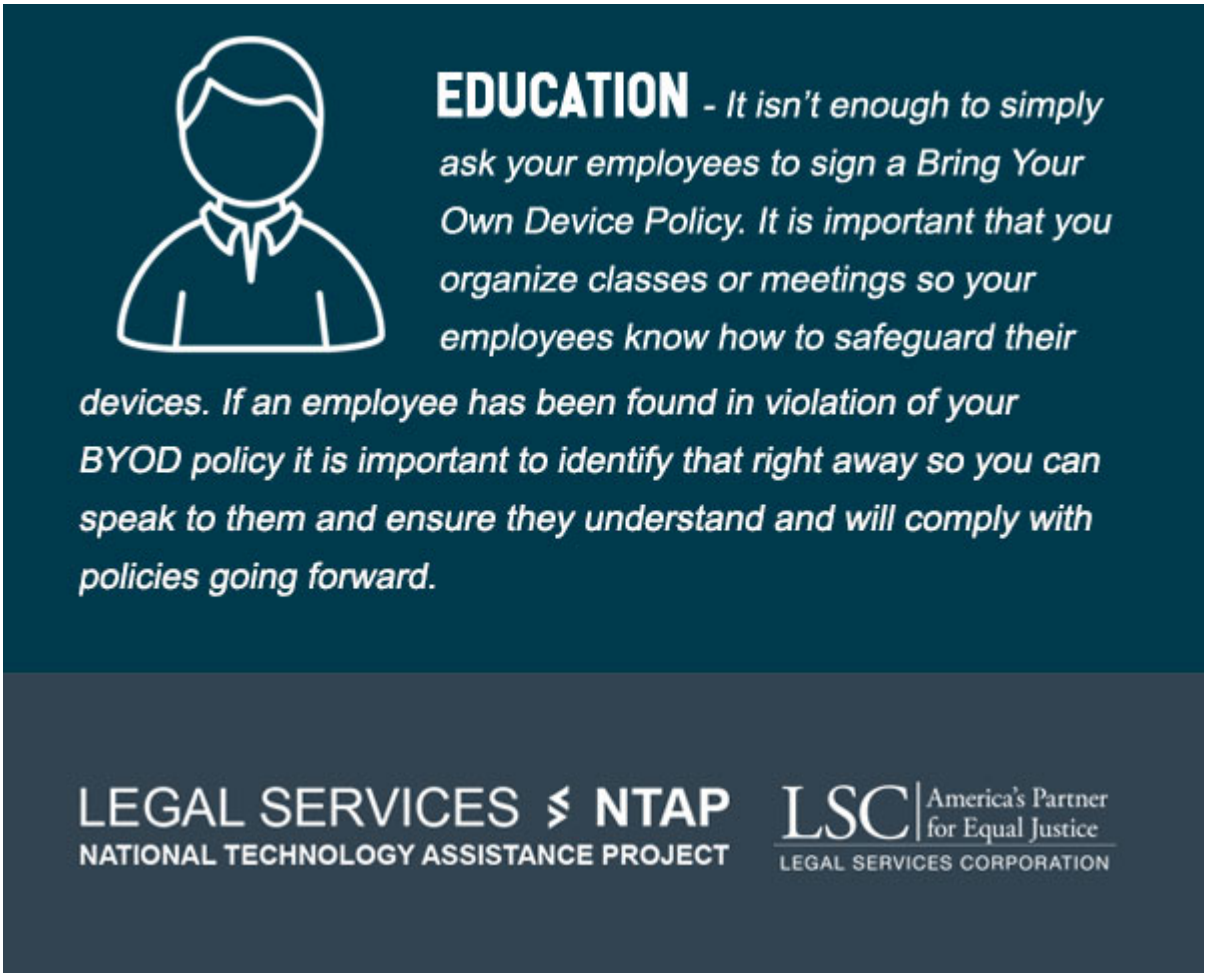
Multi Factor Authentication -

Multi-factor authentication is a security method in which a computer user is granted access only after successfully presenting two or more pieces of evidence. For example you can change your gmail settings so that when you log into your email on a new machine it will prompt you to enter a code on your phone.

PASSWORD MANAGERS - *Using tools like TrueKey or LastPass can store all your organization's passwords in one place. Essentially all your employees can sign into a password manager tool and then they will have access to all company login details which will autofill when you visit a website.*

REMOTE WIPE - *The employee's device may be remotely wiped if the device is lost or IT detects a data or policy breach. Remote wipe is a crucial safeguard against viruses or similar threats to the security of your organization's data and infrastructure.*

REMOTE DESKTOPS - *Having a remote desktop means employees can use a work computer by logging in and controlling the system through the internet. This method almost entirely prevents the possibility of an attack and is very secure.*



Last updated on January 08, 2022.

Security

Files

Bring Your Own Device Policy Info-graphic

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

10 Oct 2024

LSNTAP Announces Access to Comprehensive Technology Initiative Grants Database

Ypsilanti, MI – October 10, 2024 – Legal Services National Technology…

Continue Reading

18 Jul 2024

LSNTAP Launches a New Resource for the Community: the RFP Library

Over the last two years, LSNTAP staff has pored over the listserv archive to…

Continue Reading

Our Partners

MAP | MICHIGAN ADVOCACY PROGRAM

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION