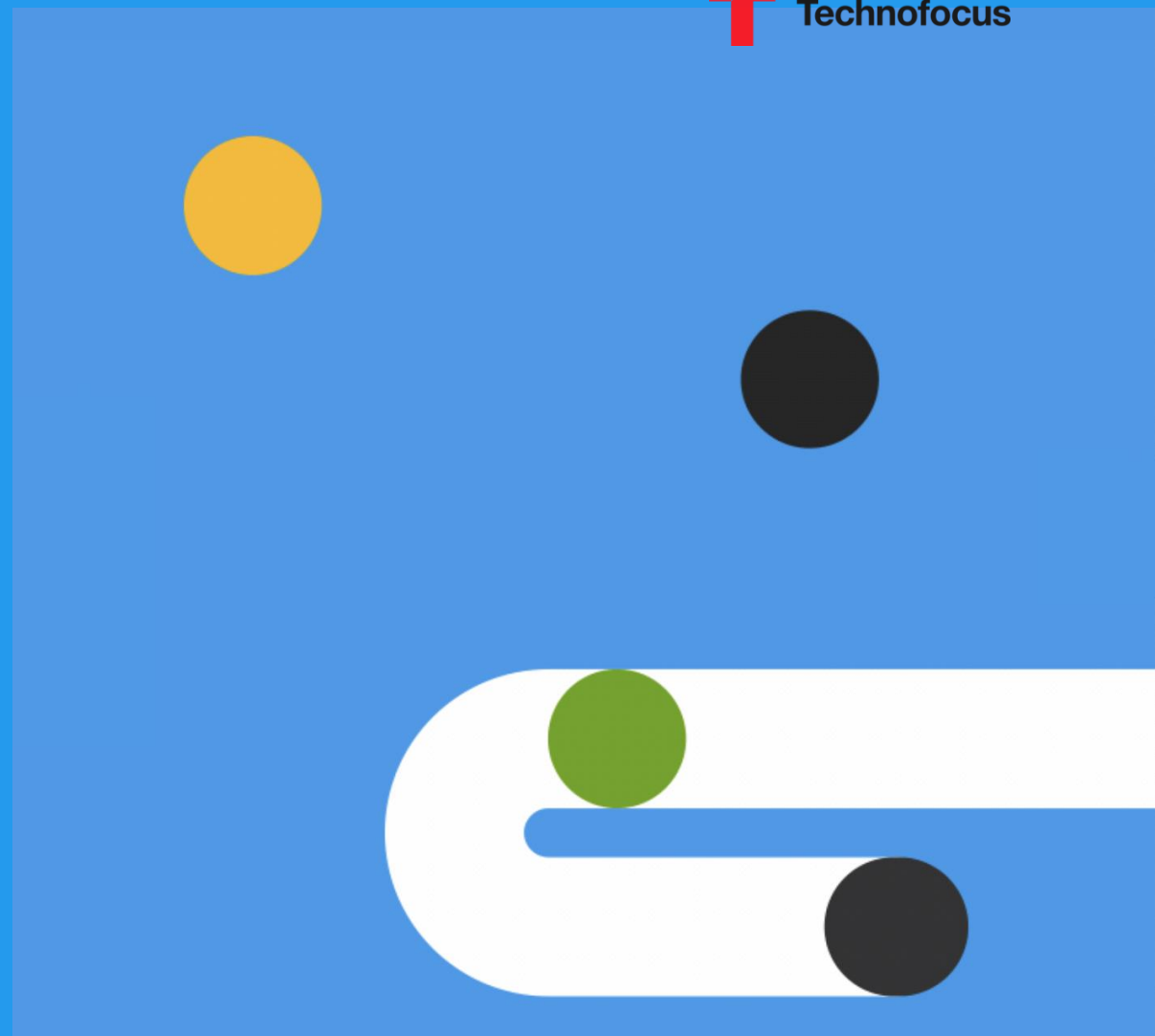


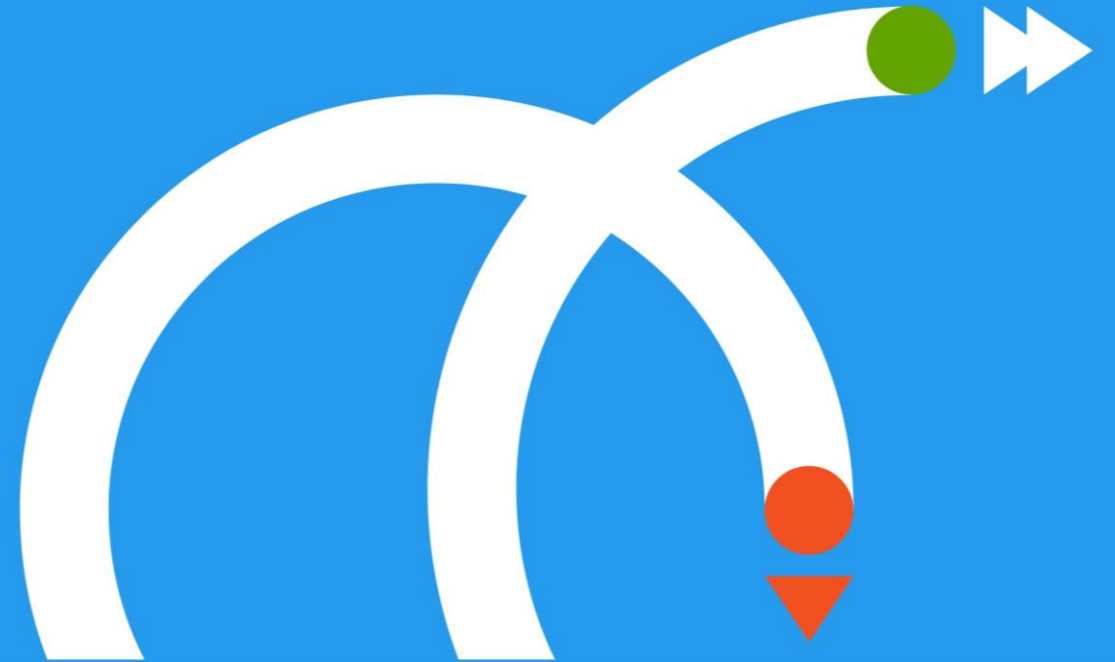
Adopting Secure user practices online

APAC | Jun 2021



Agenda

- ▶ Online Threats Overview
- ▶ Common Threats
- ▶ Data Breach
- ▶ Malware
- ▶ Phishing
- ▶ Social Engineering
- ▶ Password Safety
- ▶ Cyber Security
- ▶ Email Protection
- ▶ Preventive Measures



Introduction

Various types of security threats are increasing in number and severity

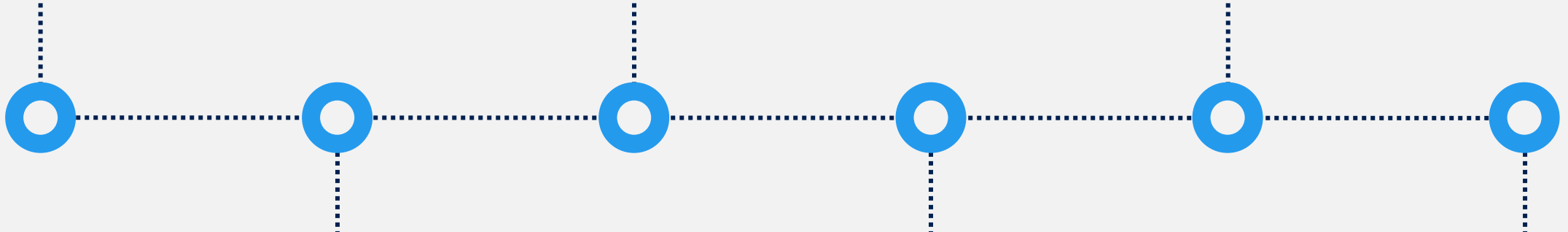
Threats are becoming more sophisticated as well-financed

Various types of security threats are increasing in number and severity

Cybercriminal gangs develop improved variants of malware and social engineering attacks

Focus on email as the primary threat vector for cybercriminal activity

Many organizational users are not exercising proper due diligence



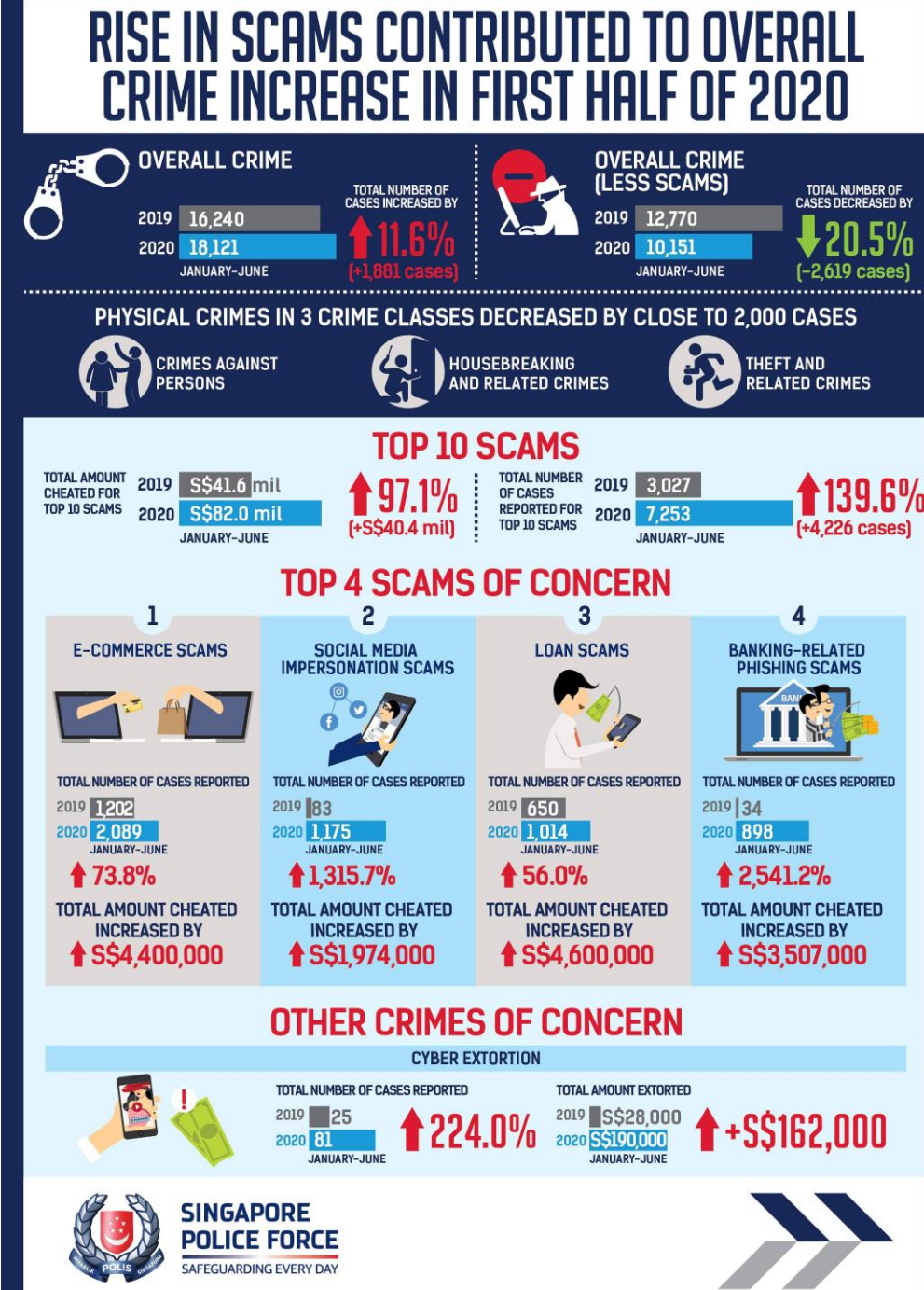
Banking-related phishing scams spike more than 2,500% in first half of 2020 in Singapore

CNA, Singapore

The scammers told the victim that his accounts have been hacked and they needed his OTPs to disable his bank accounts.

Police warned that platforms like IMO, Viber and WhatsApp were also commonly used by these scammers to communicate with their victims.

E-COMMERCE SCAMS REMAIN TOP SCAM TYPE

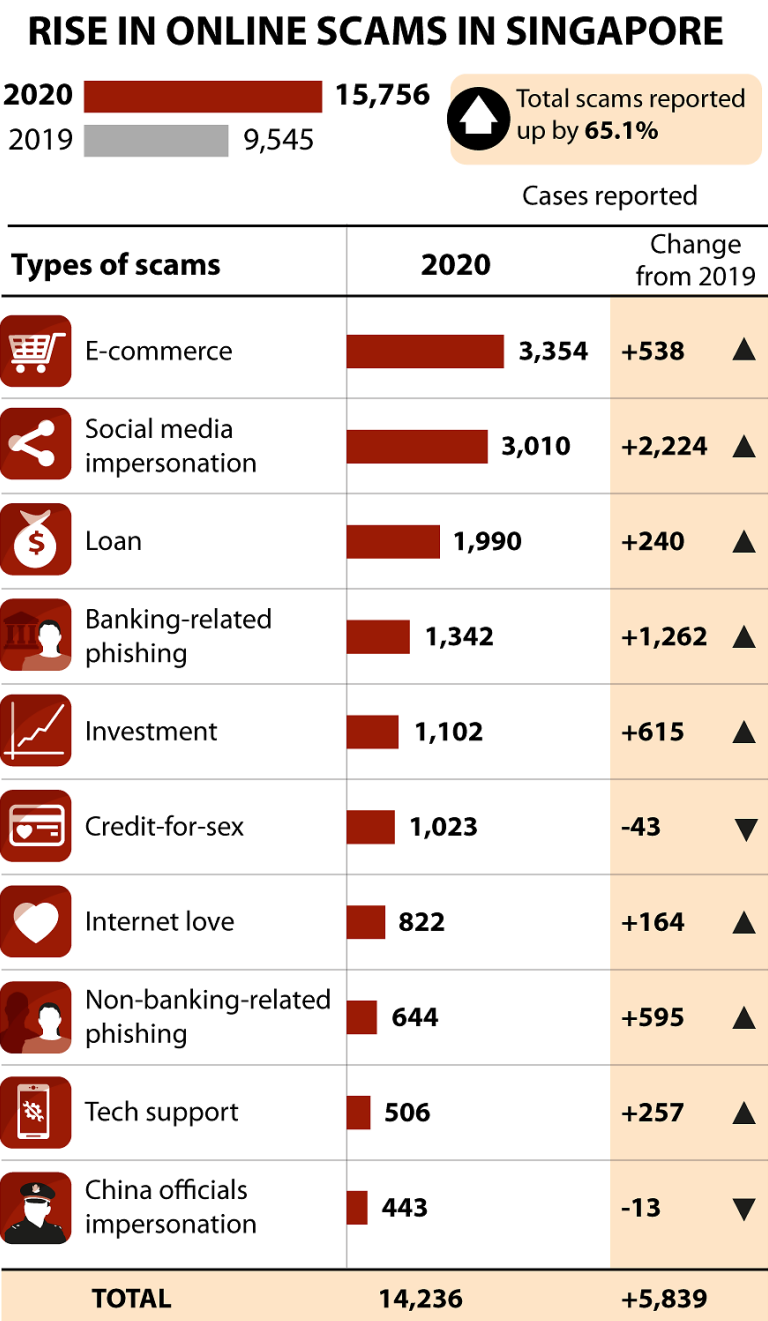


More than 180 investigated over scams involving S\$1.5 million in Singapore

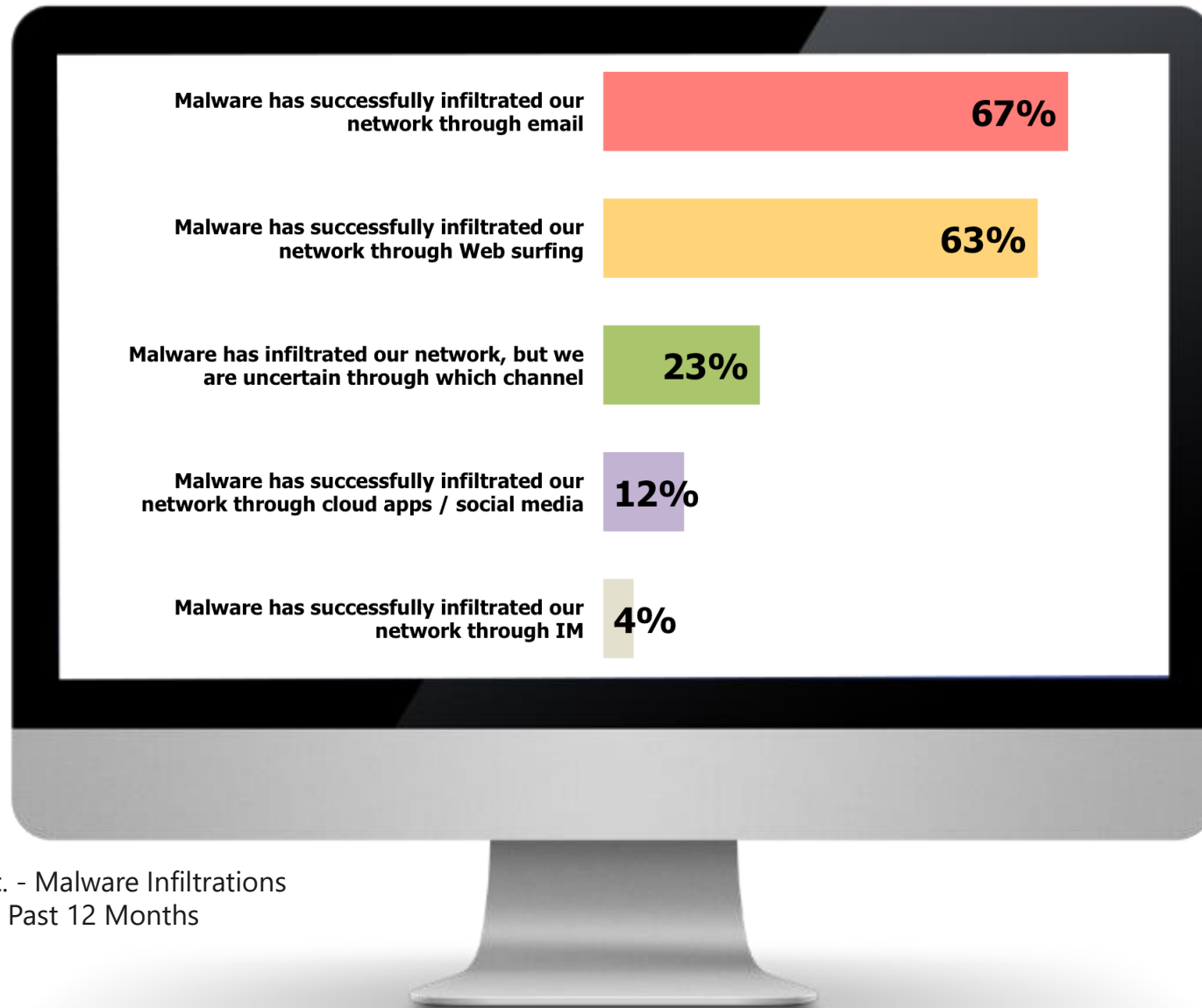
"Scammers would often claim to help their victims sign up for online contests or promotions which turned out to be fake.

"Their victims would later discover that unauthorised transactions had been made from their bank accounts or mobile wallets,"

Instagram and Facebook were the most common social media platforms where such scams took place



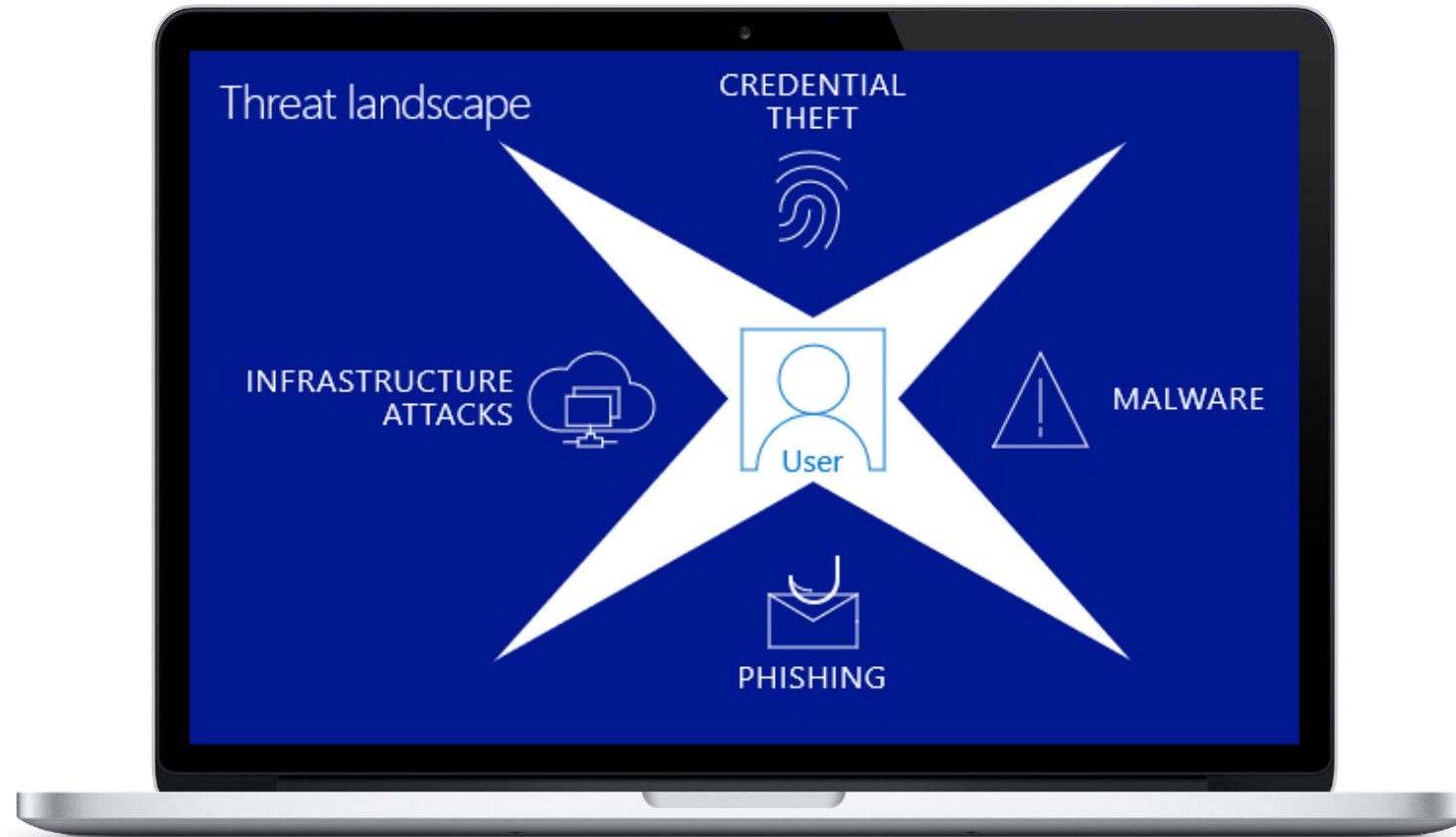
Primary Security Concerns




Source: Osterman Research, Inc. - Malware Infiltrations
That Have Occurred During the Past 12 Months

Threats Overview


Common threats



Data Breach



A data breach is a cyber attack in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion

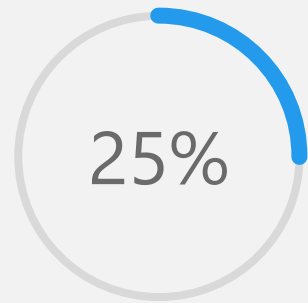


Data breaches can occur in any size organization, from small businesses to major corporations

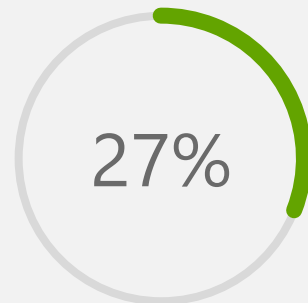
Example of data breach

- ▶ Loss or theft of hard copy notes, USB drives, computers or mobile devices
- ▶ An unauthorized person gaining access to your laptop, email account or computer network
- ▶ Sending an email with personal data to the wrong person
- ▶ A bulk email using 'to' or 'cc', but where 'bcc' (blind carbon-copy) should have been used
- ▶ A disgruntled employee copying a list of contacts for their personal use
- ▶ A break-in at the office where personnel files are kept in unlocked storage

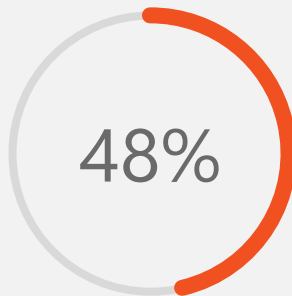
Root Cause of Data Breaches



Human Error



Process Failure



Malicious



Ponemon Institute 2016 Cost of Data Breach Study: Global Analysis

Threats Overview



Malware



Phishing

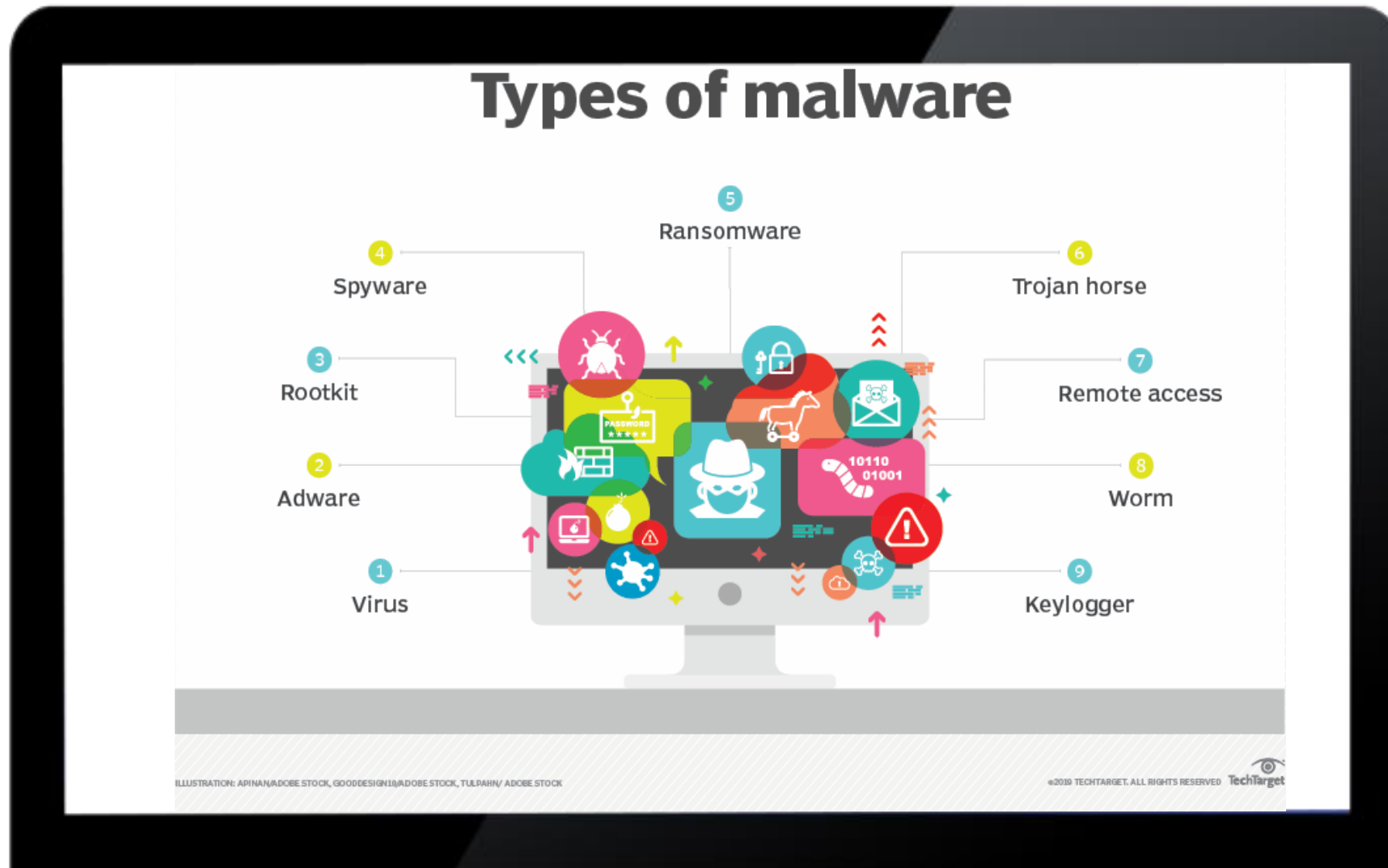


Social
Engineering

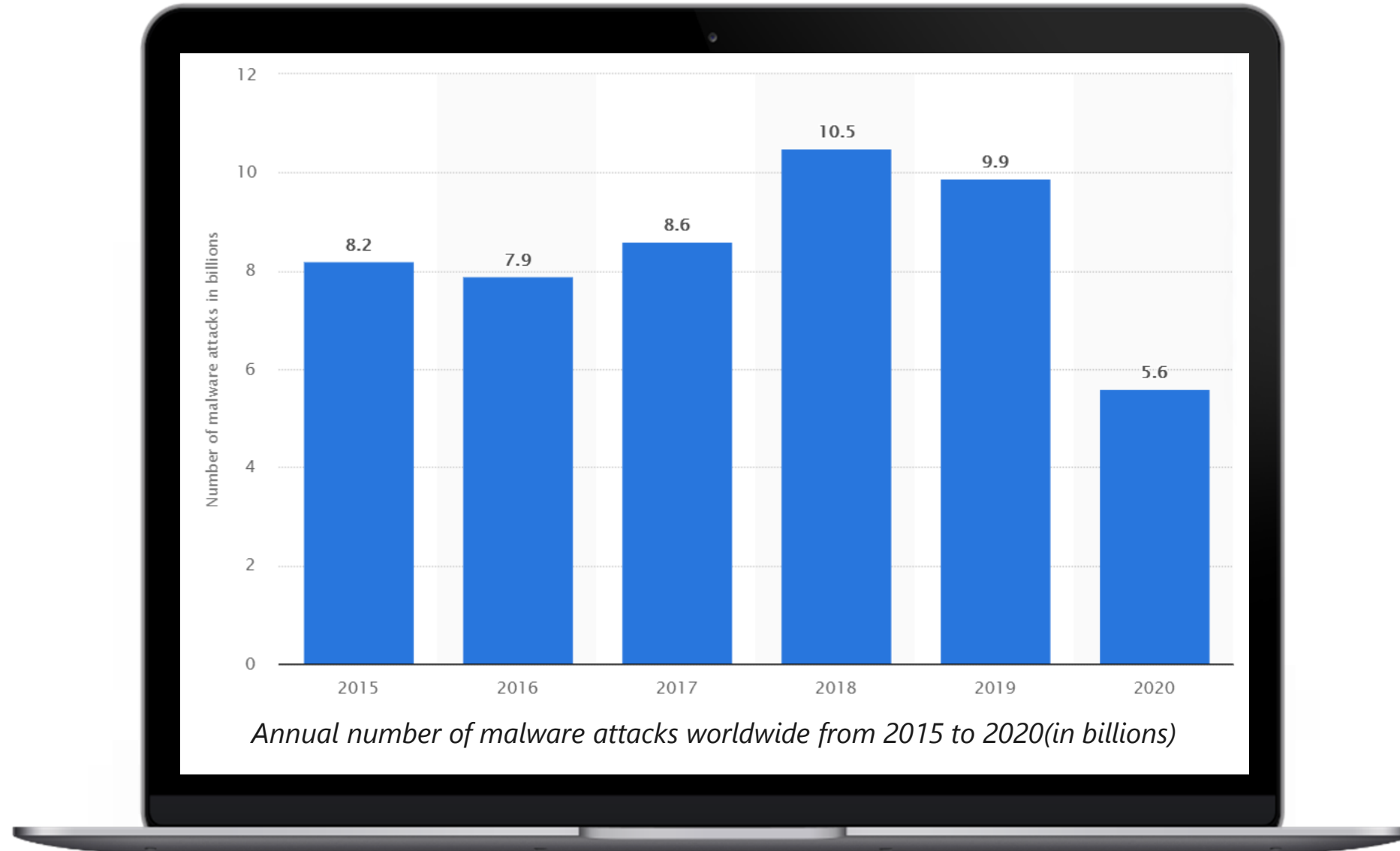
Malware

- ▶ On average, 390,000 unique threats per day
- ▶ Unique threats ≠ extremely dissimilar
- ▶ Malicious threats are changed in the smallest amount possible to evade detection
- ▶ Malicious threats are targeted in order to have the highest penetration (success) rate

Malware includes numerous threat families, all with different names

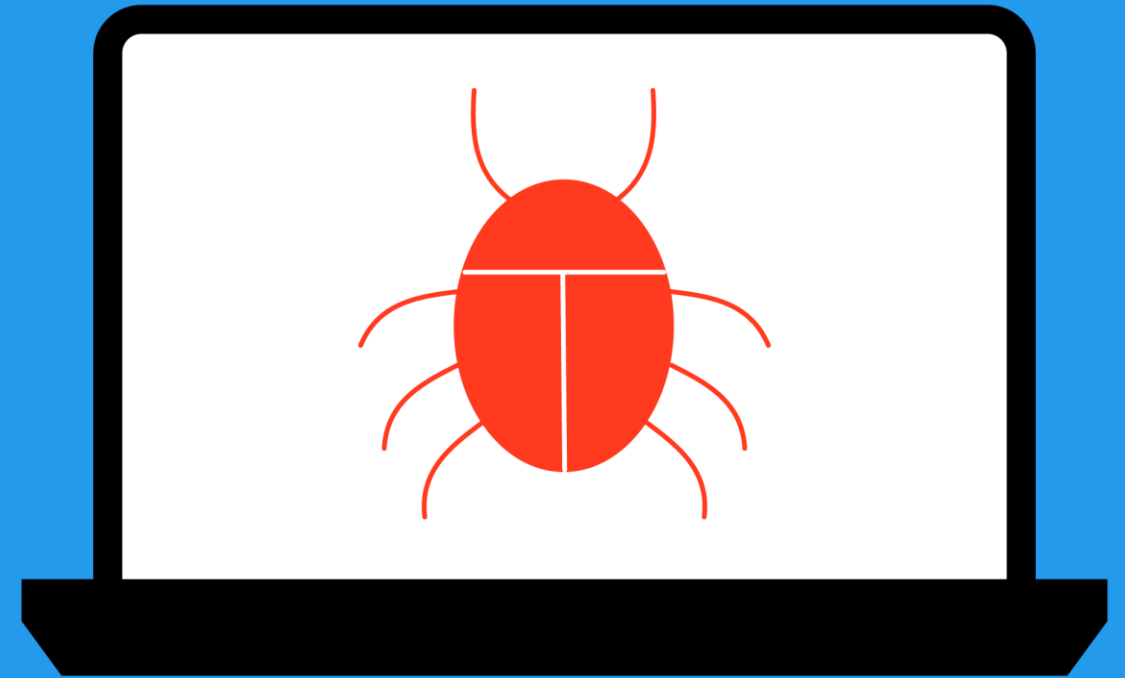


Growth of Malware



How does my computer get infected?


- ▶ Clicking malicious links in email
- ▶ Plugging in an unknown flash drive
- ▶ Downloading malware masquerading as other software




How to detect malware

- ▶ Sudden loss of disc space,
- ▶ Unusually slow speeds,
- ▶ Repeated crashes or freezes, or
- ▶ An increase in unwanted internet activity
- ▶ Pop-up advertisements

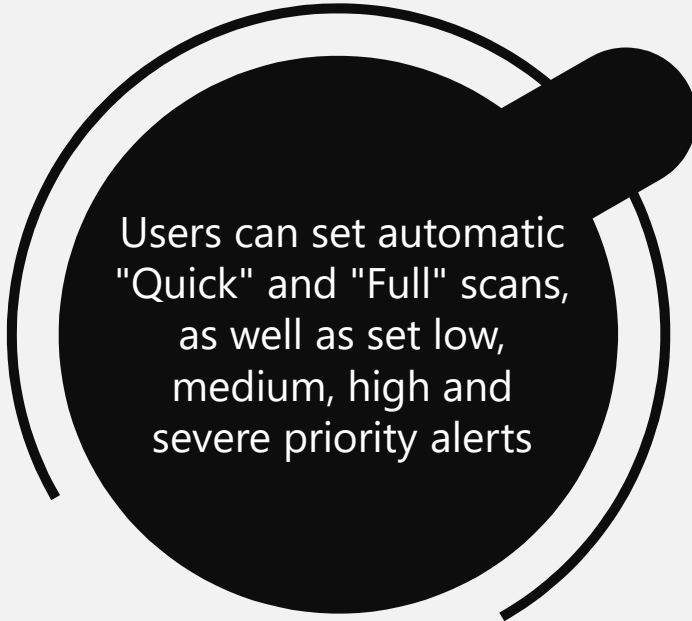
Prevent with Microsoft Windows Defender on your PC



Windows Defender is anti-malware software from Microsoft included in Windows 10 Operating system



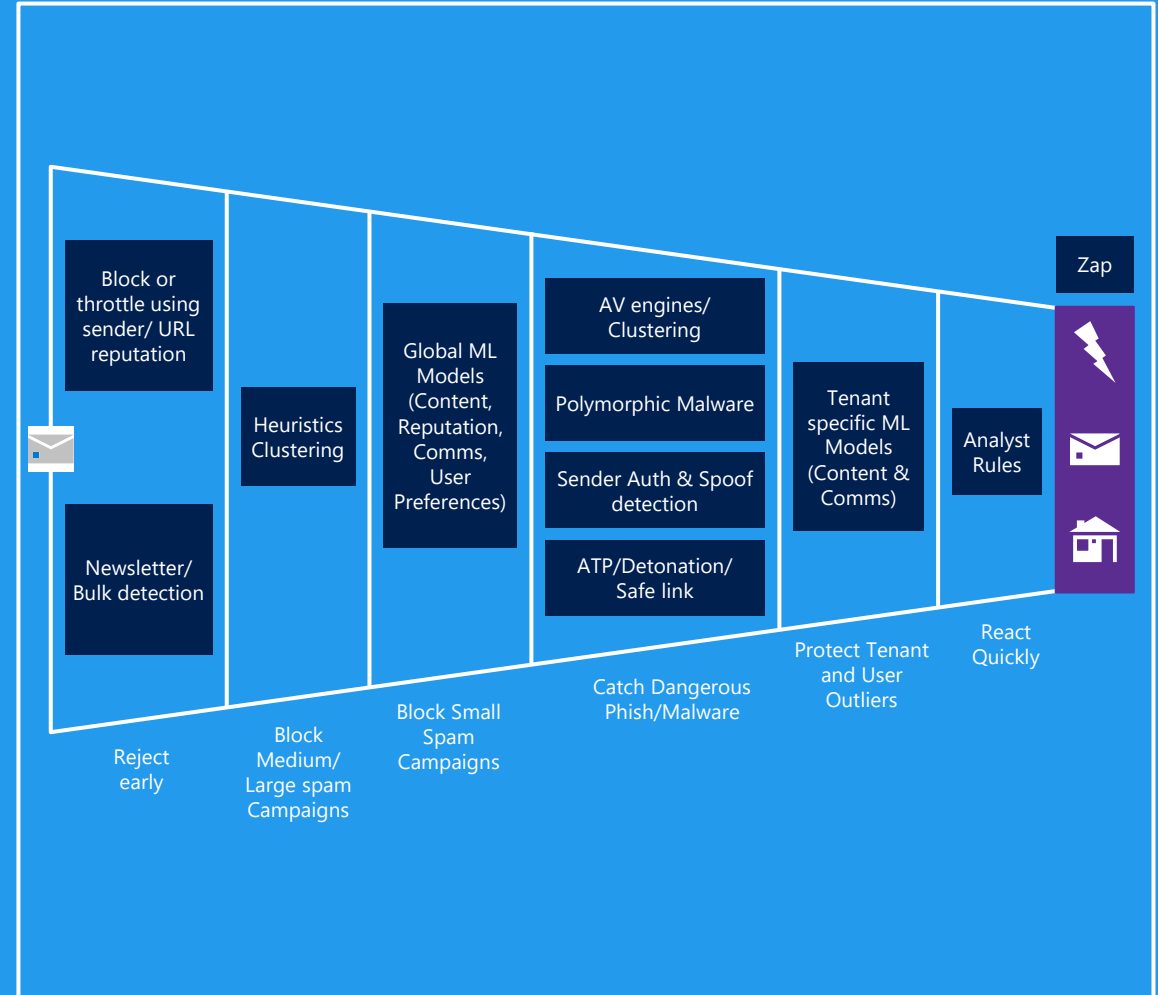
Windows Defender protects against threats such as spyware, adware and viruses.



Users can set automatic "Quick" and "Full" scans, as well as set low, medium, high and severe priority alerts

The anti-malware pipeline in Office 365

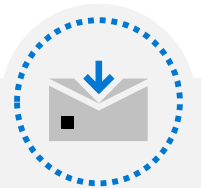
- 1 Before mail enters the Microsoft network and is processed by EOP, techniques such as IP and sender reputation, combined with heuristics
- 2 After that, it is scanned by multiple signature-based anti-virus scanners
- 3 Next, EOP scans individual files using a reputation block
- 4 Heuristic clustering is used to identify mail as suspicious simply based on an analysis of delivery patterns
- 5 Once these signals are collected, the results are run through a machine-learning (ML) model
- 6 If Microsoft Defender for Office 365 is enabled in the tenant, it extends the protection of EOP



Zero-hour auto purge (ZAP)

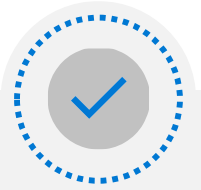


Microsoft 365 organizations with mailboxes in Exchange Online, zero-hour auto purge (ZAP) is an email protection feature that retroactively detects and neutralizes malicious phishing, spam, or malware messages that have already been delivered to Exchange Online mailboxes



The ZAP action is seamless for the user; they aren't notified if a message is detected and moved

Phishing and spoofing protection



By design, the SMTP protocol supports spoofing

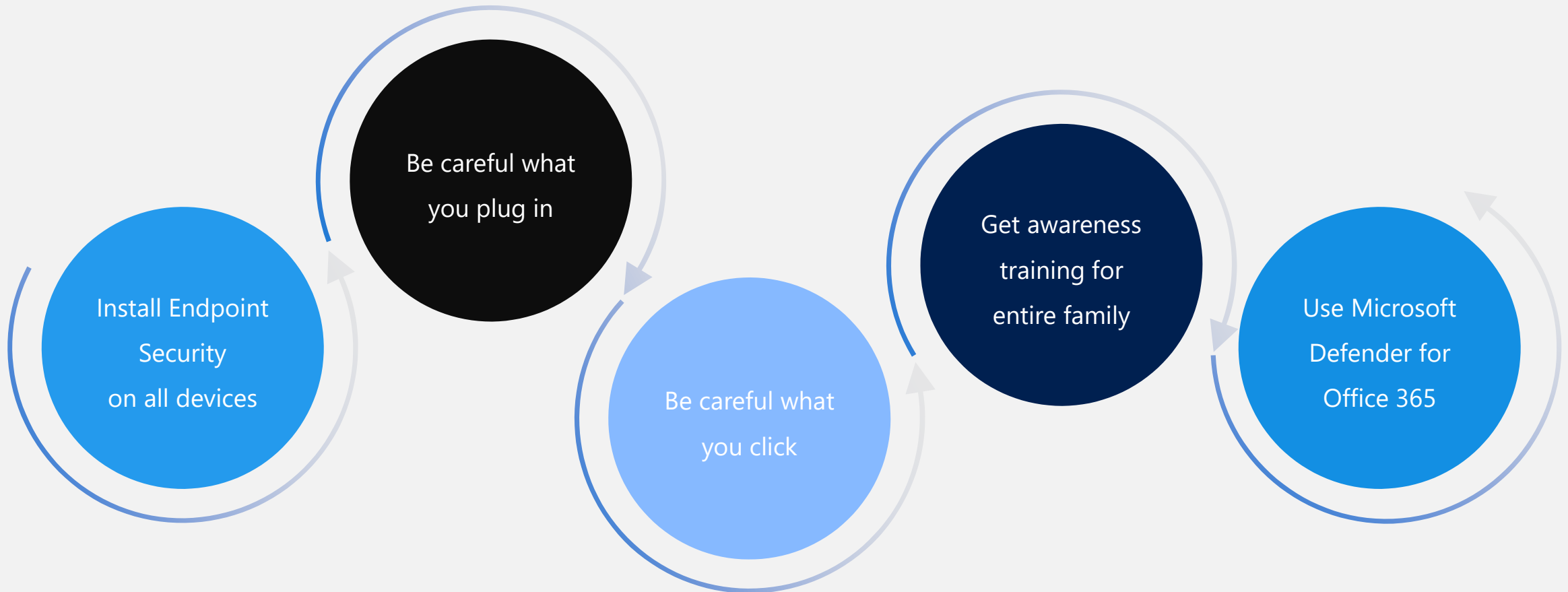


EOP has built-in anti-spoofing and anti-phishing protection designed to detect legitimate cases of spoofing while shielding organizations from the illegitimate ones



EOP supports email authentication techniques including Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message and Reporting Compliance (DMARC)

Top Tips to Avoid Malware

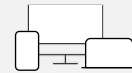
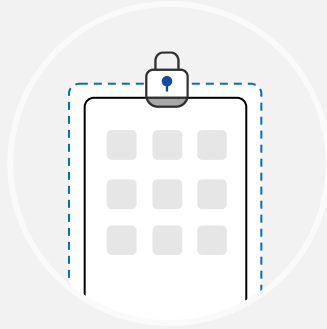


Enroll your Mobile Devices (Samsung Galaxy/iOS) in your organization MDM solution

Mobile Device Management (MDM)

Conditional Access:

Restrict access to managed and compliant devices



Enroll devices for management



Provision settings, certs, profiles



Report & measure device compliance

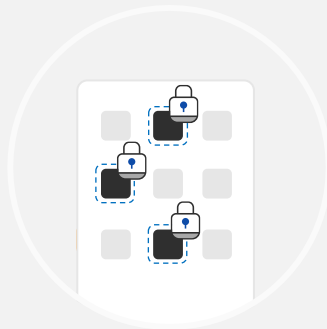


Remove corporate data from devices

Mobile Application Management (MAM)

Conditional Access:

Restrict which apps can be used to access email or files



Publish mobile apps to users



Configure and update apps




Report app inventory & usage




Secure & remove corporate data within mobile apps


Phishing



Intentionally
deceiving someone
by posing as a
legitimate company



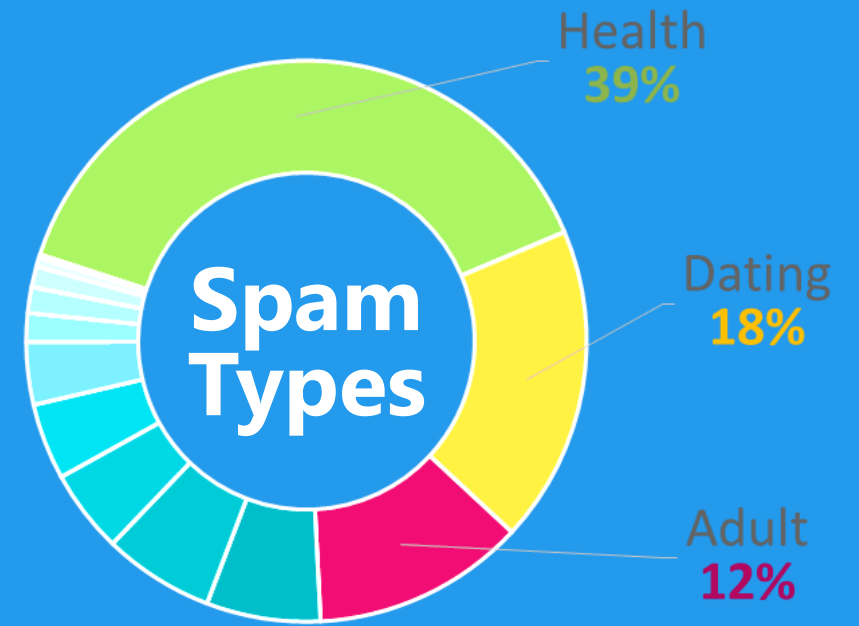
Typically, utilizes
email by pretending
to be a company or
service requesting
you to do something



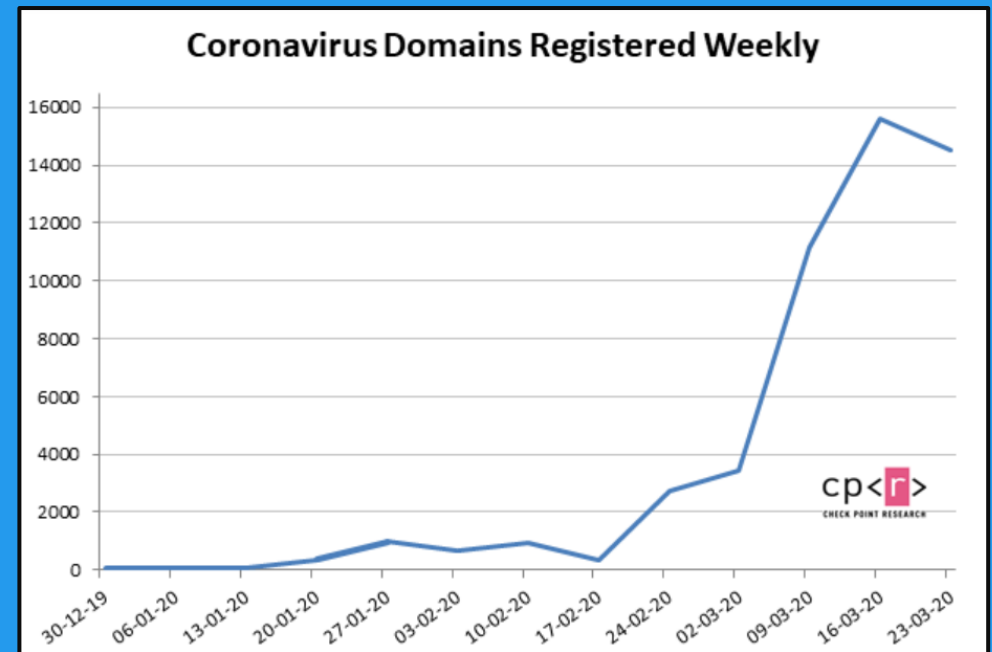
Hoping that you click
the link and fill out
the requested info

Phishing Stats

- ▶ 54% of all inbound email is spam
- ▶ 1 in 20 email messages has malicious content

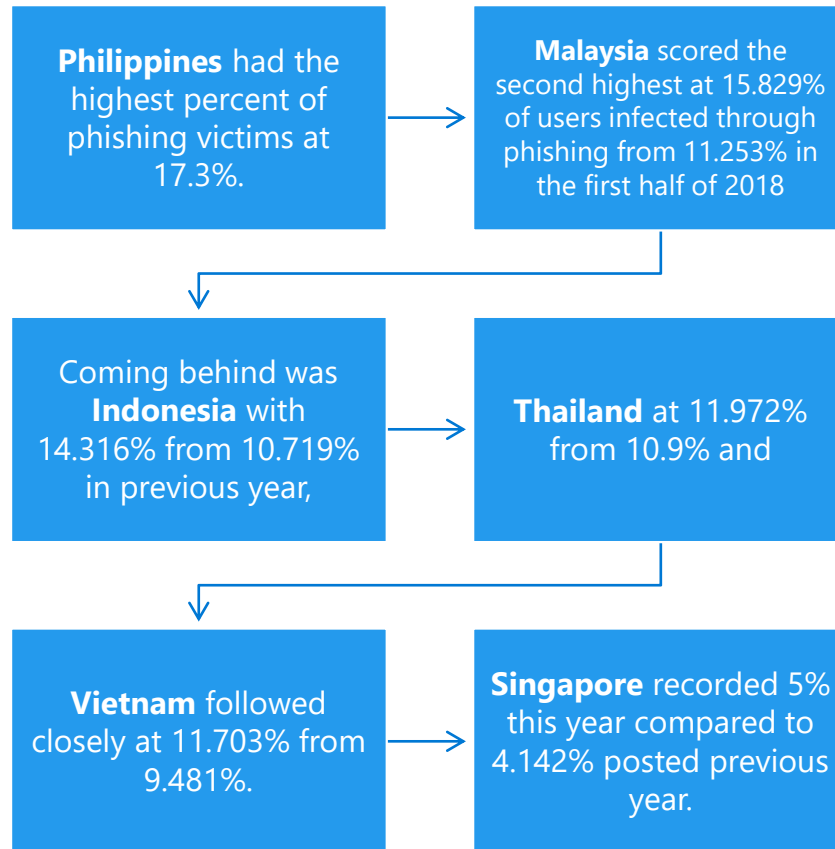


2016 Trustwave Global Security Report

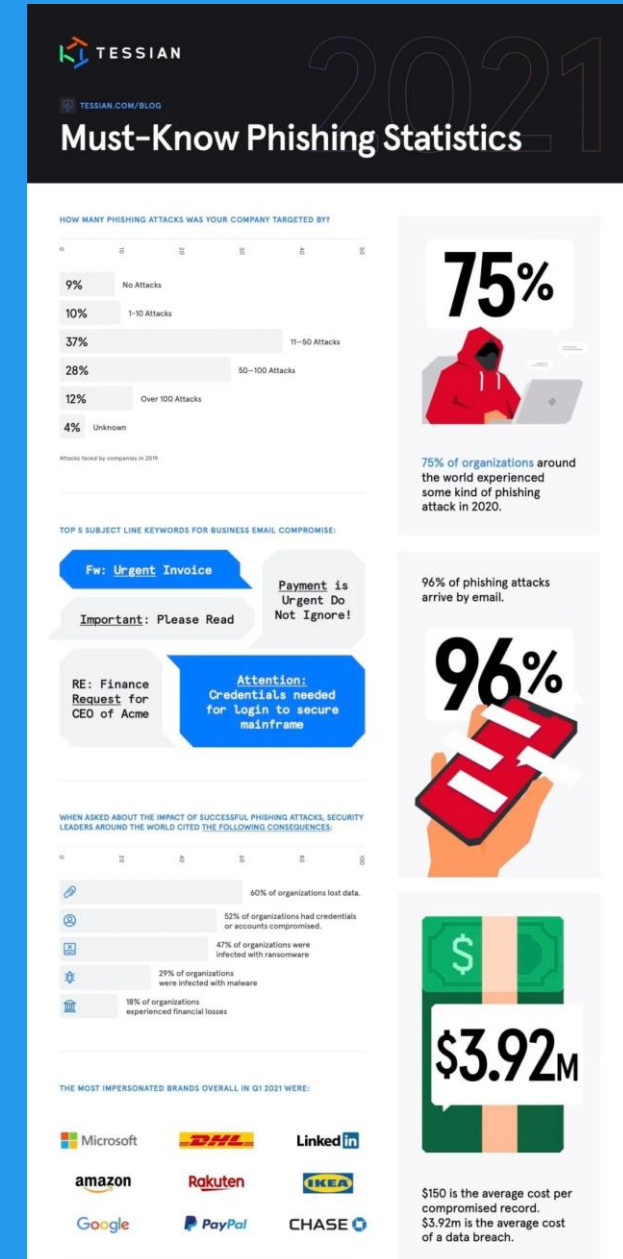


Southeast Asia a hotbed for phishing attacks

During the first half of 2019



Source: <https://securitybrief.asia/story/southeast-asia-a-hotbed-for-phishing-attacks>



Phishing Examples

----- Forwarded Message -----

From: PayPal <paypal@notice-access-273.com>

To:

Sent: Wednesday, January 25, 2017 10:13 AM

Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

[Help](#) | [Contact](#) | [Security](#)

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

Not
paypal.com

Phishing Examples

The image shows a screenshot of a PayPal account page titled "Account Limited". The page is designed to look like the official PayPal interface, with a top navigation bar containing links for Summary, Activity, Send & Request, Wallet, Shop, and a Log Out button. The main content area is divided into two columns. The left column contains two boxes: "What can I do while my account is limited?" with a list of allowed actions (update account info, use PayPal logos) and "What can't I do while my account is limited?" with a list of restricted actions (send/receive money, withdraw money, close account, link/remove cards/bank accounts, dispute transactions, send refunds). Below these is a "Secured & Certificate by" section featuring three logos: VeriSign Identity Protection, 100% Secure, and Symantec Validation & ID Protection. A red arrow points to these logos. The right column has a heading "Account Limited" and three icons for Account Login, Update Address, and Card Information. Below these is a yellow warning box with an exclamation mark icon and the text "Complete the steps listed to restore your account access." This is followed by a form with fields for Address Line 1, Address Line 2, City, State, ZIP / Post Code, Country (set to United States), Phone Number, Mother's Maiden Name, Social Security Number, and Date of Birth. A red arrow points to the "Mother's Maiden Name" field, and another red arrow points to the "Social Security Number" field. The "Date of Birth" field has dropdown menus for month, day, and year.

PayPal Summary Activity Send & Request Wallet Shop Log Out

What can I do while my account is limited?

- ✓ update your account information
- ✓ use PayPal logos in your auction listings or on your website

What can't I do while my account is limited?

- ✗ send or receive money
- ✗ withdraw money from your account
- ✗ close your account
- ✗ link or remove a card
- ✗ link or remove a bank account
- ✗ dispute a transaction
- ✗ send refunds

Secured & Certificate by

VeriSign Identity Protection 100% Secure Symantec Validation & ID Protection

Account Limited

Account Login Update Address Card Information

Complete the steps listed to restore your account access.

Address Line 1 :

Address Line 2 :

City :

State :

ZIP / Post Code :

Country :

Phone Number :

Use for fraud alert.

Mother's Maiden Name :

For security reason, Please enter your correct information.

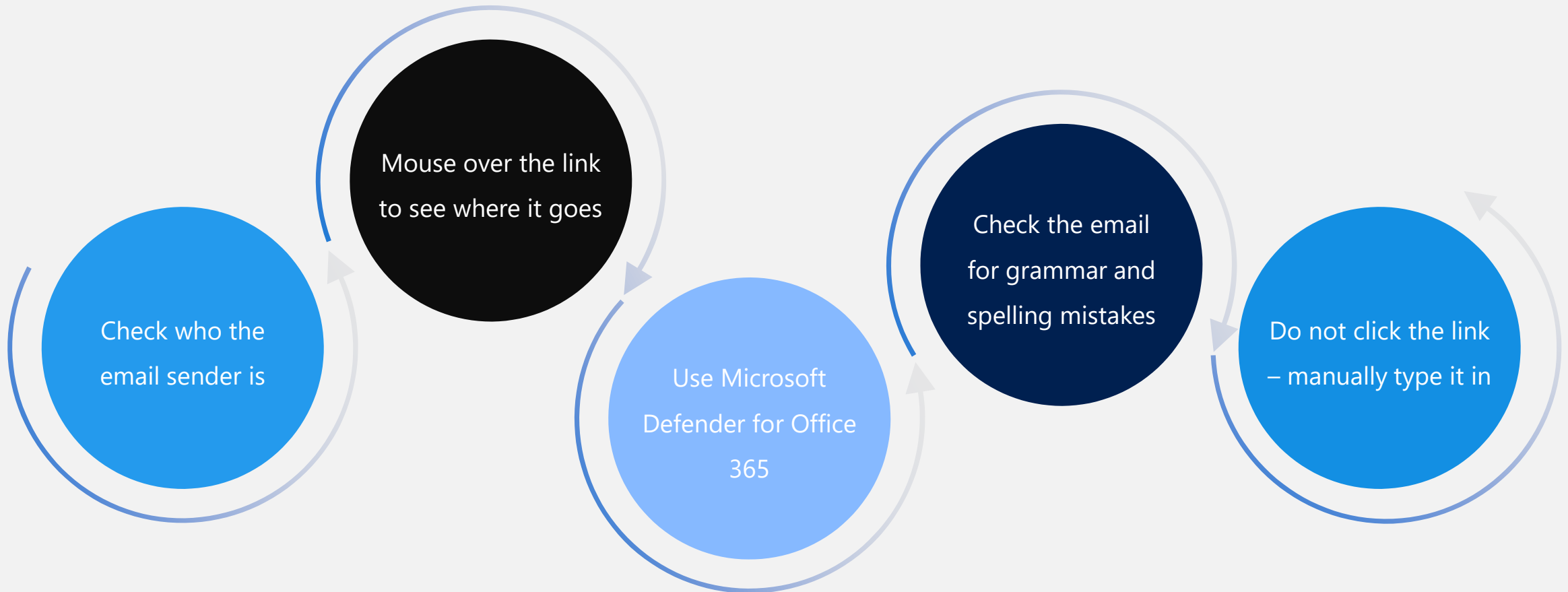
Same tax ID as on your tax return

Social Security Number : - -

We'll confirm.

Date of Birth :

Top Tips to Avoid Phishing

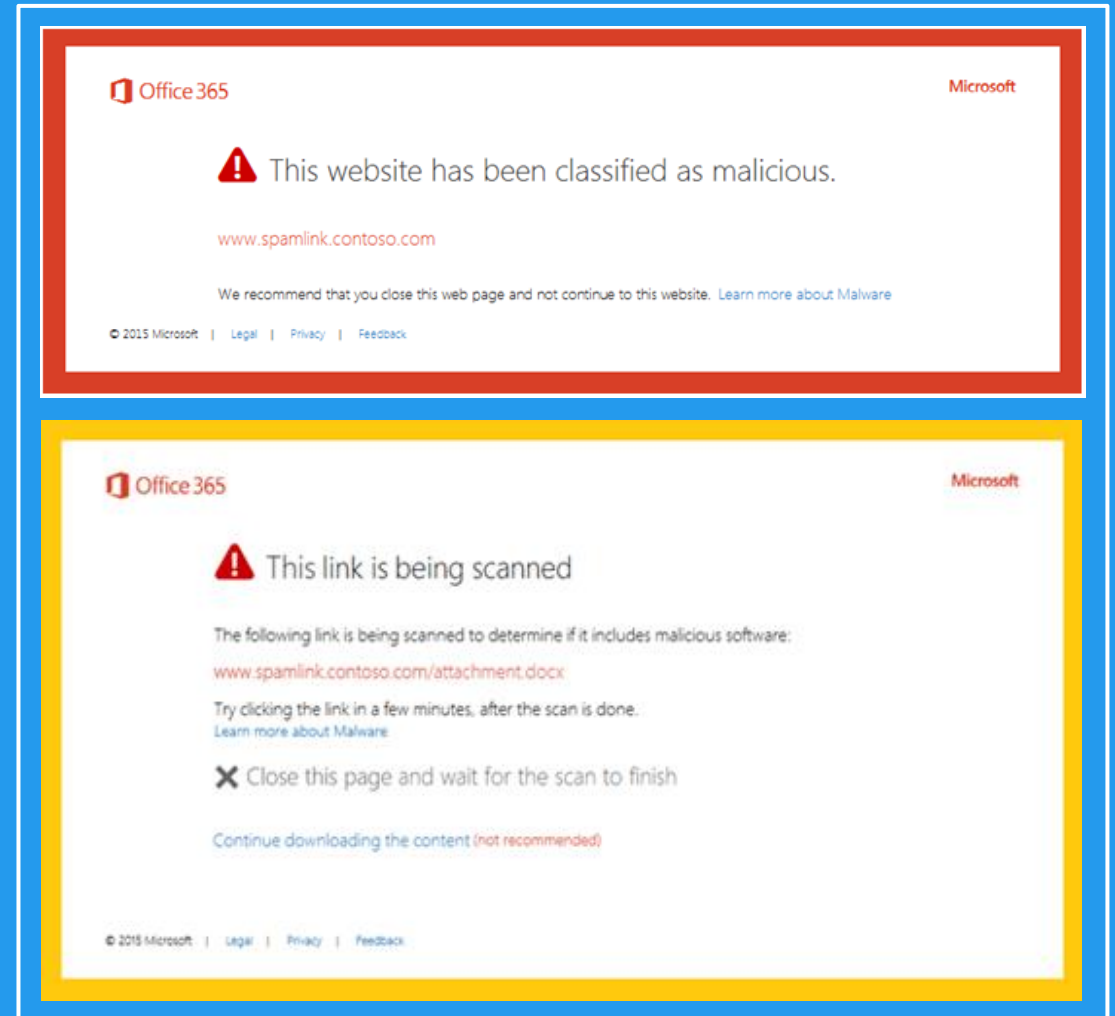


Safe Links in email in Outlook

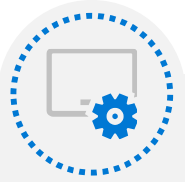
Safe Links is a feature in Microsoft Defender for Office 365 that protects users from malicious URLs by providing time-of-click verification of web addresses

When a user clicks a link in a message or document, Safe Links checks to see if the link is malicious by redirecting the URL to a secure server in the Microsoft 365 environment that checks the URL against a block list of known malicious web sites

Exchange Online Protection also scans each message in transit in Office 365 and provides time of delivery protection, blocking any malicious hyperlinks in a message



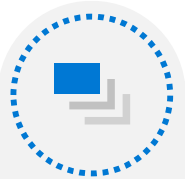
Safe Attachments in MS Outlook



Safe Attachments is a feature in Microsoft Defender for Office 365 that opens every attachment of a supported file type in a special hypervisor environment, checks to see if the attachment is malicious, and then takes appropriate action



Safe Attachments will analyze attachments that are common targets for malicious content



Selecting attachments to test



Attachment testing



Safe Attachments example

Demo

Safe Attachments

Demo

Safe Links

Social engineering

Social Engineering Attack Lifecycle



Social Engineering

- ▶ Social engineering manipulates people into performing actions or divulging confidential information
- ▶ Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems



Social engineering attack techniques

Baiting

uses a false promise to pique a victim's greed or curiosity

Scareware

involves victims being bombarded with false alarms and fictitious threats

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies

Phishing

email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims

Spear phishing

more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises

Prevention

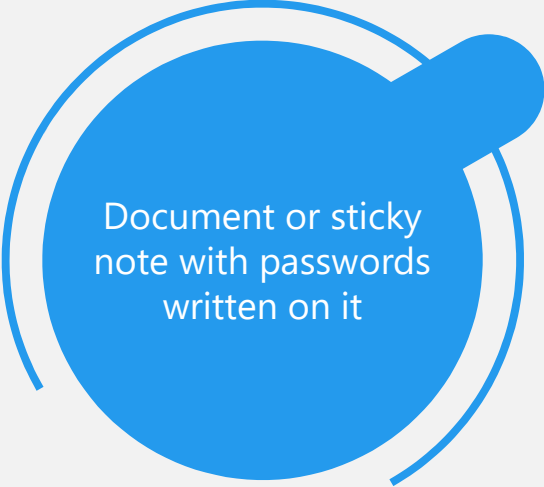
- ▶ Don't open emails and attachments from suspicious sources
- ▶ Use multifactor authentication
- ▶ Be wary of tempting offers
- ▶ Keep your antivirus/antimalware software updated

Break – 20 mins


Password Safety

Poor Password Hygiene

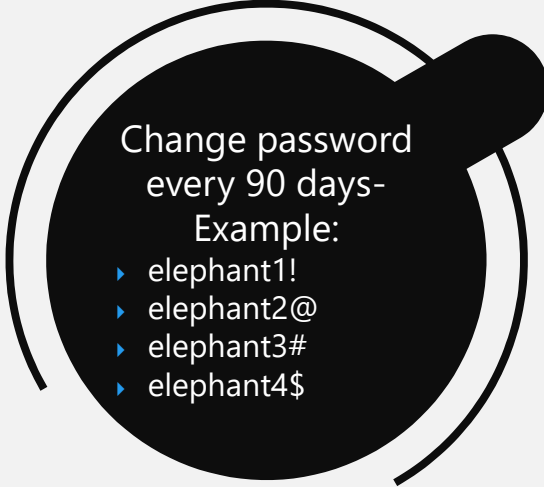
- ▶ Typically, users practice risky behavior with respect to passwords
- ▶ Passwords nowadays can be a gateway into identity theft



Document or sticky note with passwords written on it



Freely sharing password with friends, family members, colleagues



Change password every 90 days-

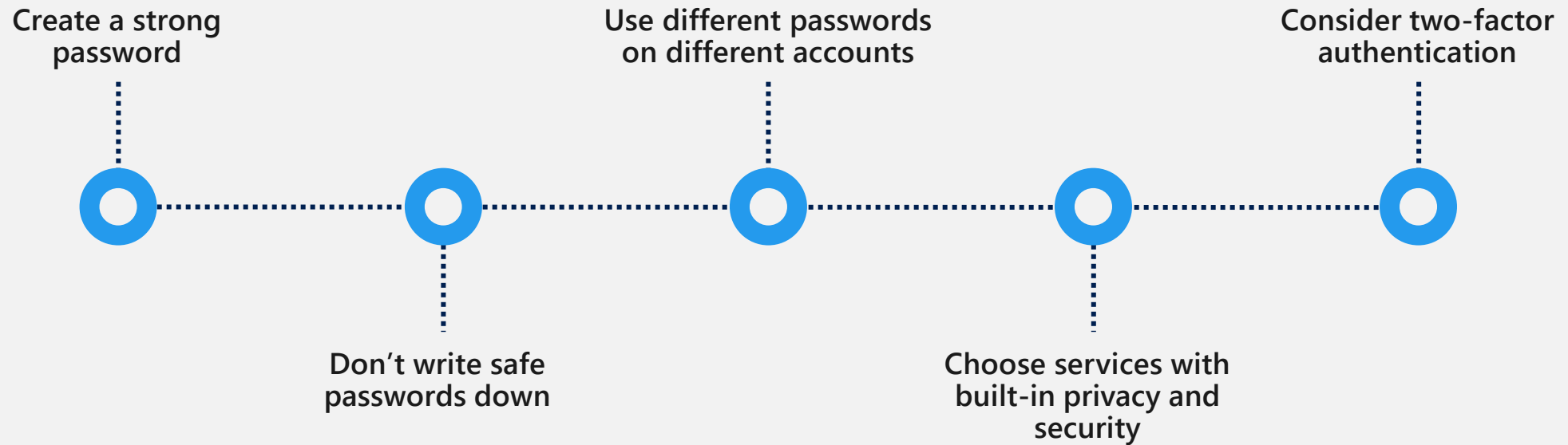
Example:

- ▶ elephant1!
- ▶ elephant2@
- ▶ elephant3#
- ▶ elephant4\$

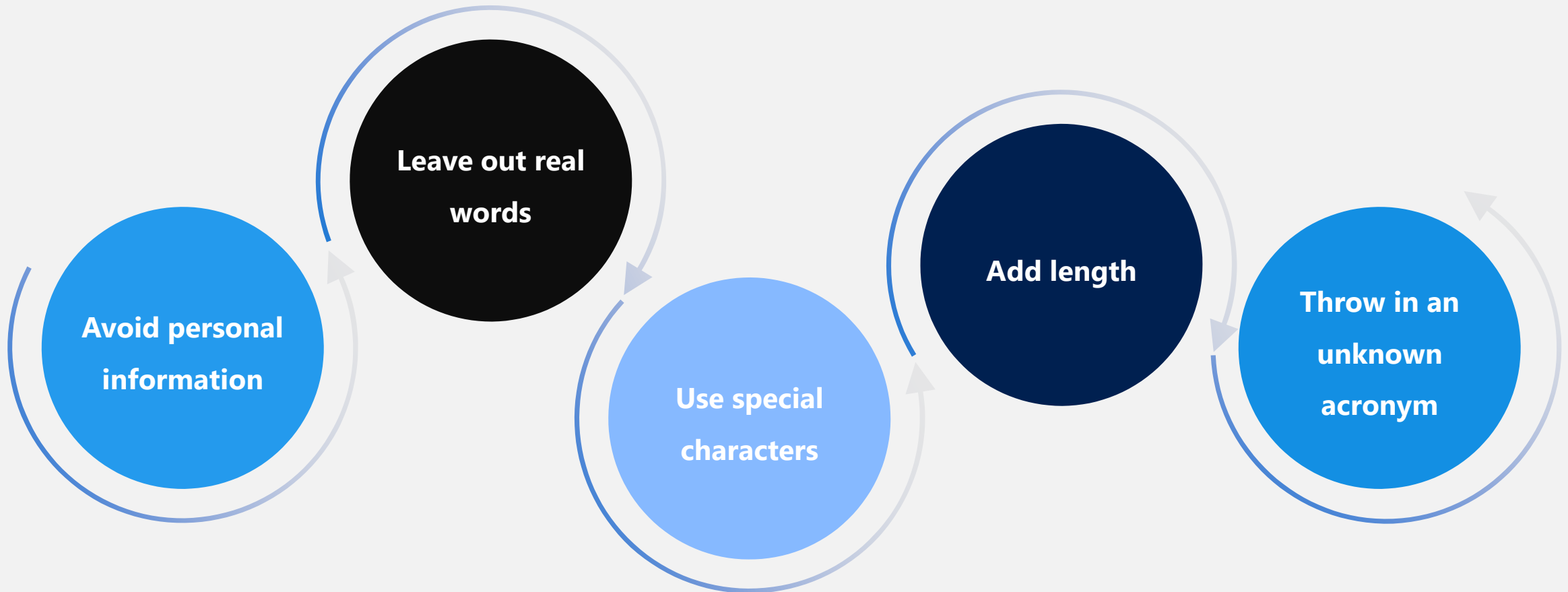
Security Questions



Password management: protection and ease of use



Creating a strong password



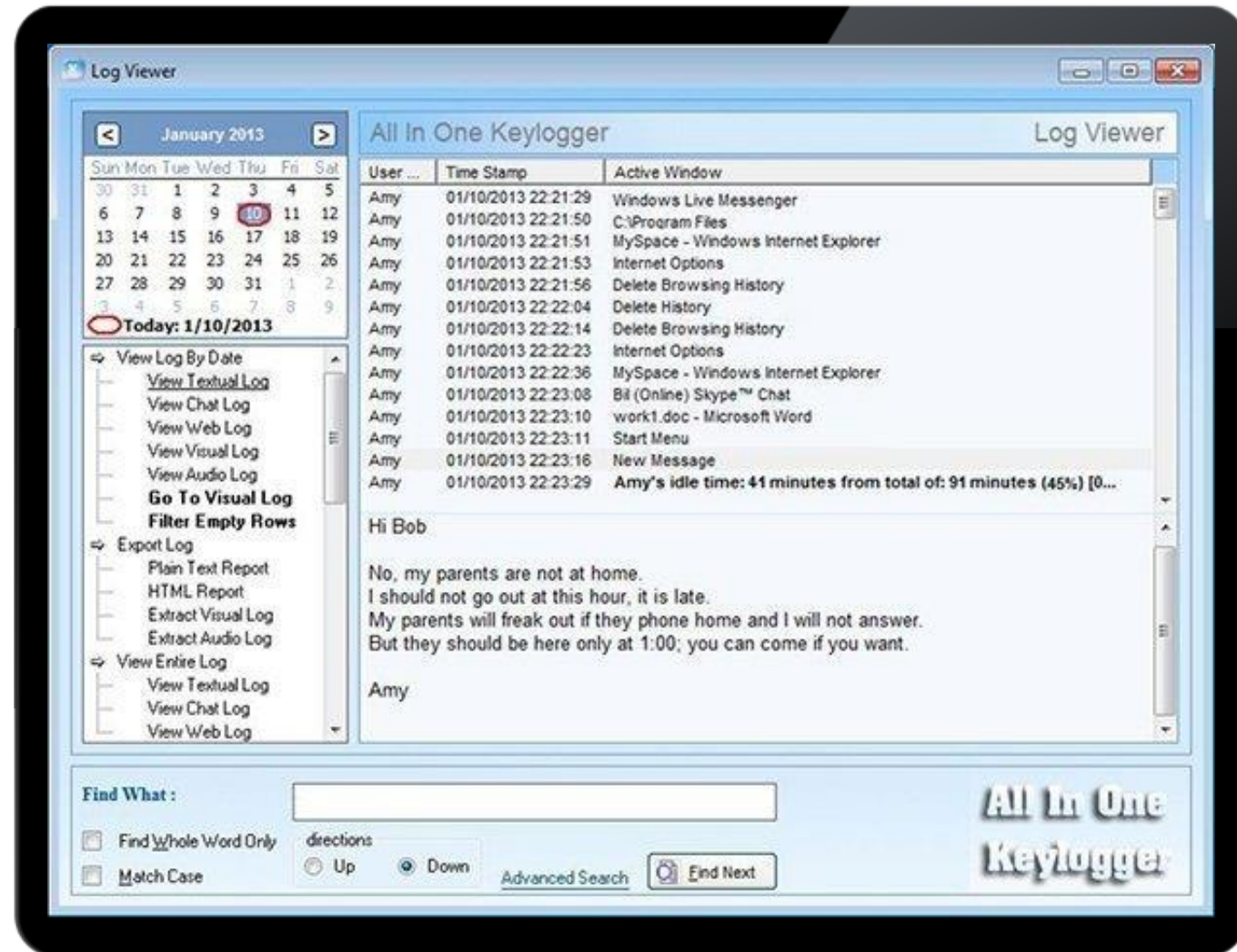
Keylogger

- ▶ A type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard
- ▶ Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data

Ethical Use cases

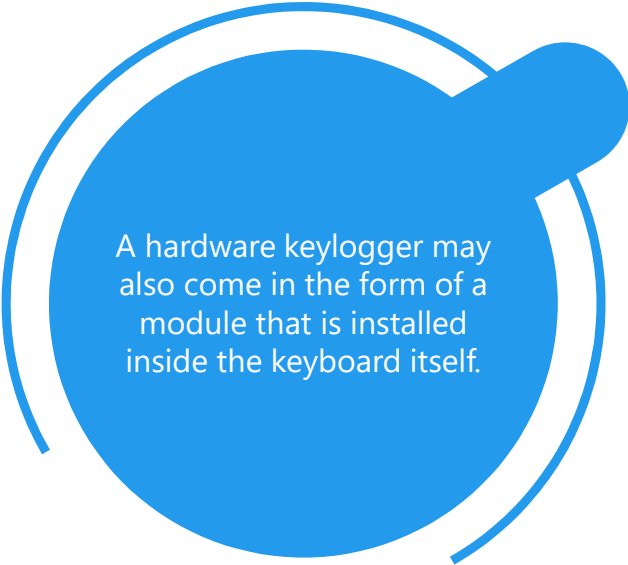
Keylogger recorders may be used by:

- ▶ employers to observe employees' computer activities
- ▶ parents to supervise their children's internet usage
- ▶ device owners to track possible unauthorized activity on their devices
- ▶ law enforcement agencies to analyze incidents involving computer use

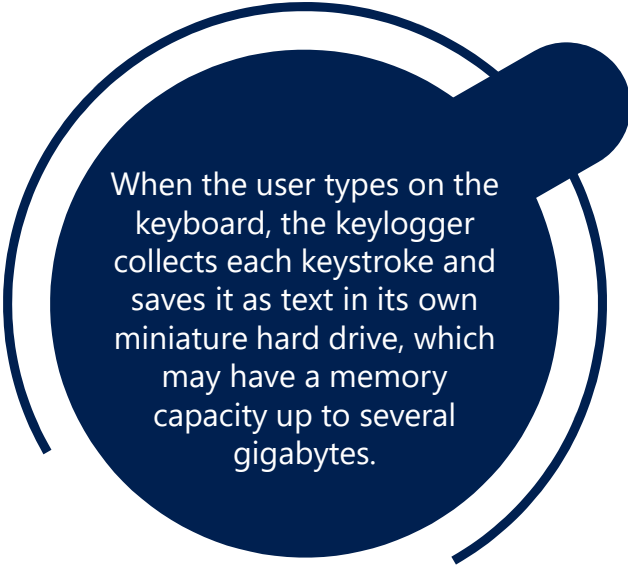


How do keyloggers work?

Hardware and software keyloggers will work differently due to their medium.



A hardware keylogger may also come in the form of a module that is installed inside the keyboard itself.



When the user types on the keyboard, the keylogger collects each keystroke and saves it as text in its own miniature hard drive, which may have a memory capacity up to several gigabytes.

The software keylogger program records each keystroke the user types and periodically uploads the information over the internet to whoever installed the program

Protection against keyloggers

- ▶ Individuals can use a **firewall** to help protect against a keylogger
- ▶ **System cages** that prevent access to or tampering with USB and PS/2 ports can be added to the user's desktop setup
- ▶ Extra precautions include using a security token as part of **two-factor authentication (2FA)** to ensure an attacker cannot use a stolen password alone to log in to a user's account, or using an **onscreen keyboard** and **voice-to-text software** to circumvent using a physical keyboard



Office 365 Services with built-in privacy and security

Security Features

Encryption of your files at rest and in transit

Monitoring for suspicious activity

Detecting ransomware

Scanning of downloads for known threats

Two-factor authentication (2FA)

When you use two-factor authentication, you will have to enter extra information when you log into your account. In most cases, this information will come from:

Prior knowledge

An account may ask for a PIN you already know or answers to a secret question you created

A tool or item you own

An account may send your phone a one-time security code for you to enter

Your being

Advanced tools may need to review your voice or face to confirm your identity

Two-factor authentication capabilities

2FA solves the problem of:

- ▶ Data breach through weak or stolen passwords
- ▶ User-created passwords that are not random characters
- ▶ Re-use of passwords intended for access to company assets for private accounts
- ▶ Passwords containing user-specific data – e.g. name, date of birth
- ▶ Simple patterns to derive new passwords, such as “elephant1,” “elephant2,” etc.

Microsoft MFA: Supported authentication methods



Mobile app
verification



Call to a
phone

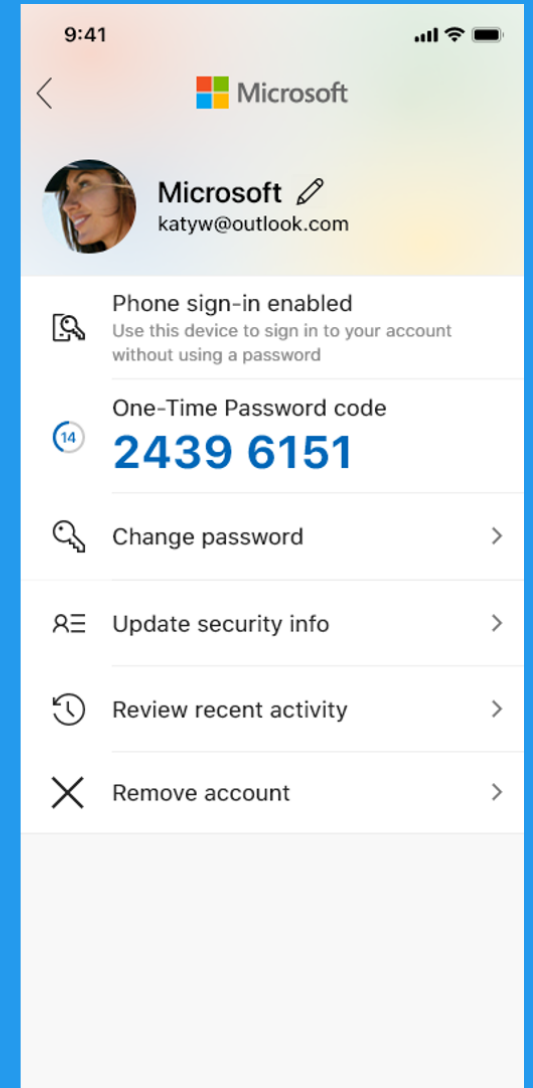
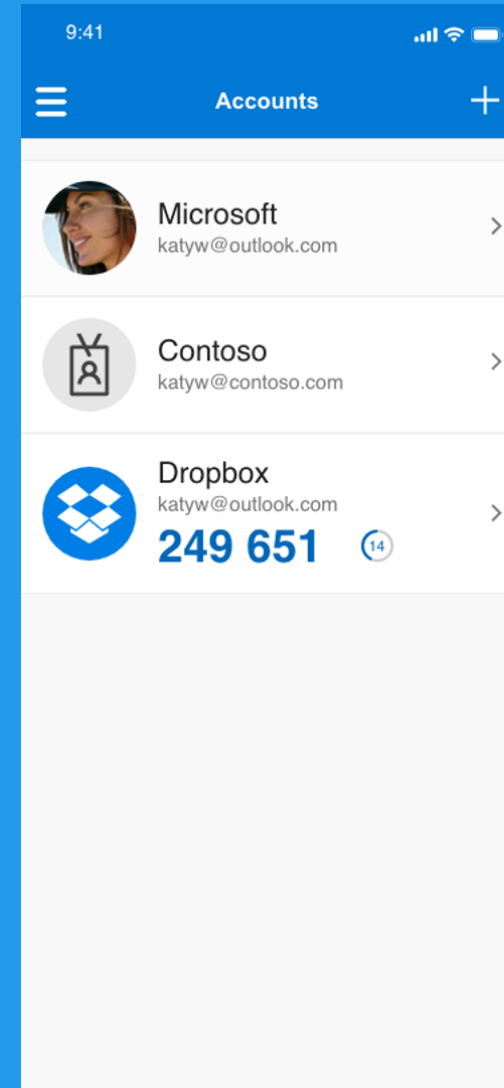


Text message
to a phone

Microsoft Authenticator app

The Microsoft Authenticator app is available for Android and iOS

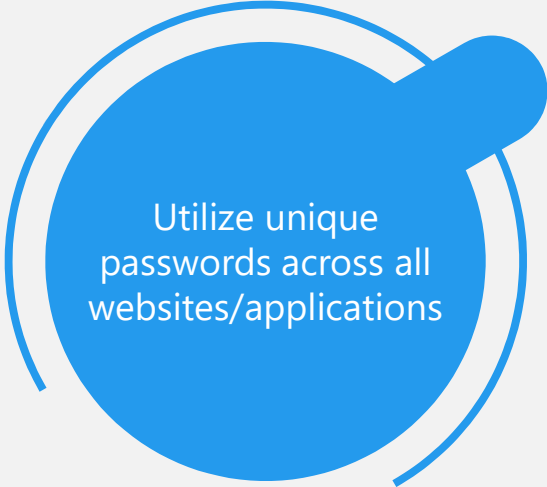
- ▶ Sign in securely without a password
- ▶ Use two-step verification for more security
- ▶ Use time-based, one-time passcodes




Demo

Using Microsoft Authenticator App to set up MFA


Tips for Password Safety



Utilize unique
passwords across all
websites/applications




Enable and
utilize 2FA on
all websites that
allow it




Choose unique,
non-true security
questions


Password Managers



If you have trouble remembering passwords or creating unique passwords, utilize a password manager



There are several very secure password managers on the market that work across all OS

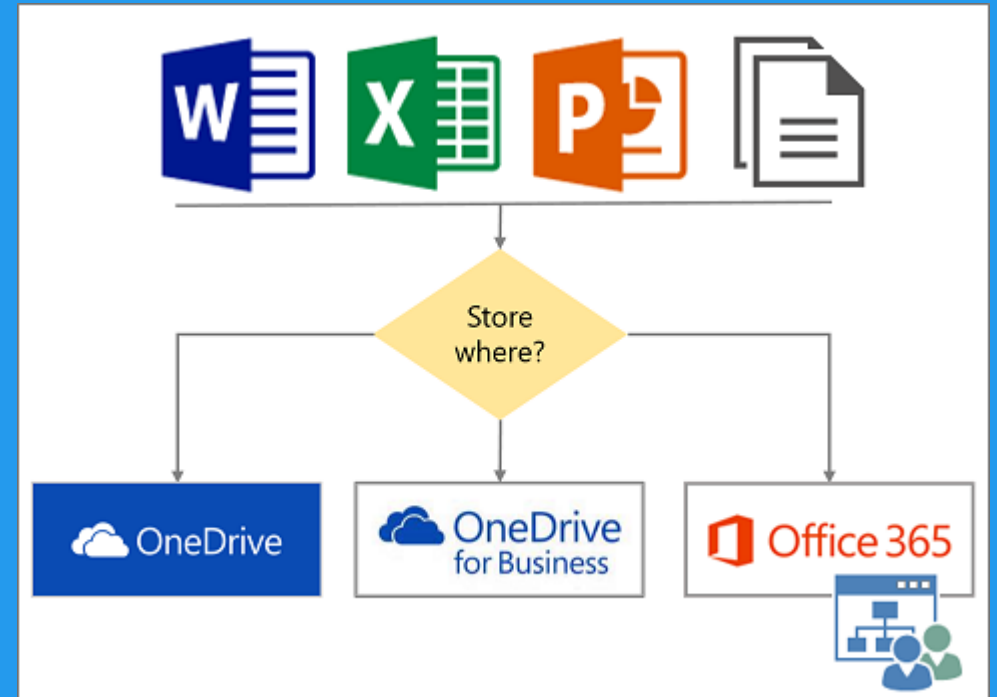


They will remember and auto-complete your passwords for you once your "master" password is entered

Cyber Security

Protect documents in the cloud

- ▶ Is your hard drive cluttered with company files and documents? These documents are at risk if your device is damaged, stolen, lost
- ▶ Save files in OneDrive or SharePoint to access them from any device
- ▶ Only those granted permission can access documents
- ▶ At any time, you can allow or revoke editing permissions for your files in the cloud



Secure your device

Block suspicious email senders

- ▶ You'll prevent possible phishing attacks, information leaks, malware, and more

Set your computer to lock after inactivity

- ▶ Any open documents are available to passersby if you don't lock your device

Run virus scans

- ▶ Maintain a healthy system by regularly checking for viruses or malware

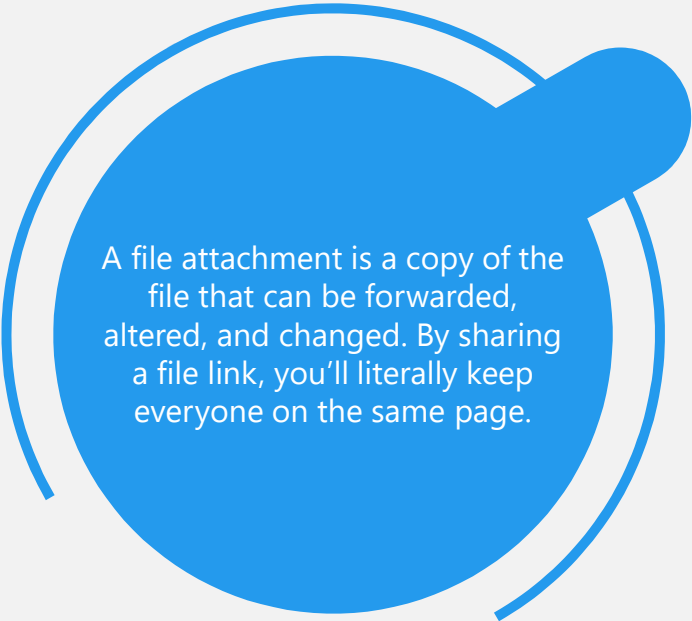
Enable computer updates

- ▶ Don't ignore security and system update notices. Instead, schedule them ahead of time

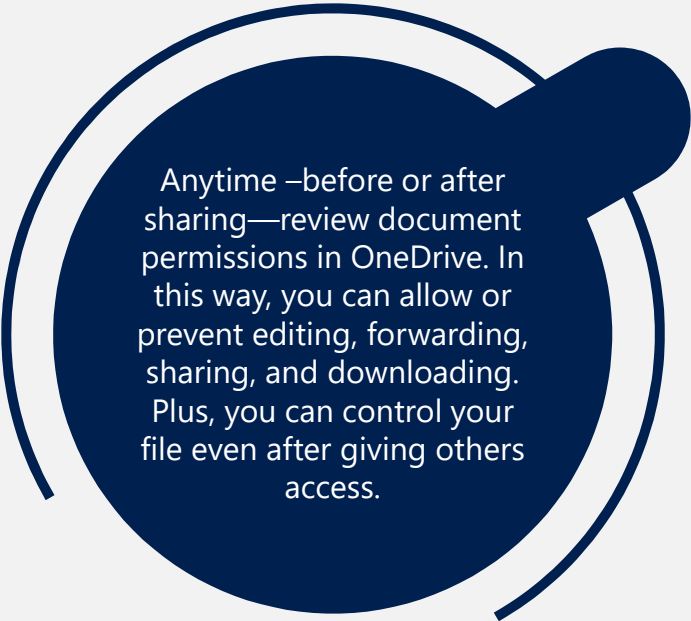
Restart your machine regularly

- ▶ This allows your computer to reset, which is a critical step if your operating system is running slow, if RAM is filling up, or if a driver crashes


Collaborate safely with colleagues



A file attachment is a copy of the file that can be forwarded, altered, and changed. By sharing a file link, you'll literally keep everyone on the same page.

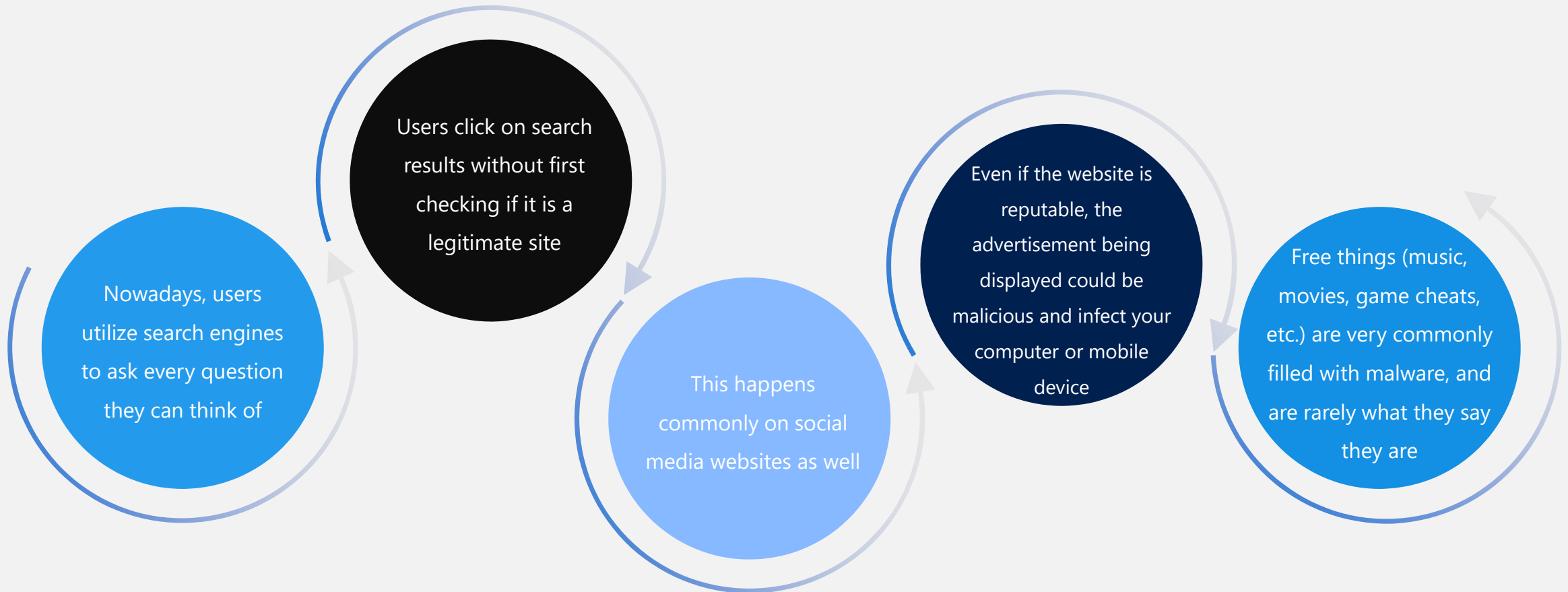


Anytime –before or after sharing—review document permissions in OneDrive. In this way, you can allow or prevent editing, forwarding, sharing, and downloading. Plus, you can control your file even after giving others access.



You can also set up rights management to protect shared documents from accidental or unauthorized changes. Restrict changes by password, person, or make it a read-only document.

Search Engine Safety



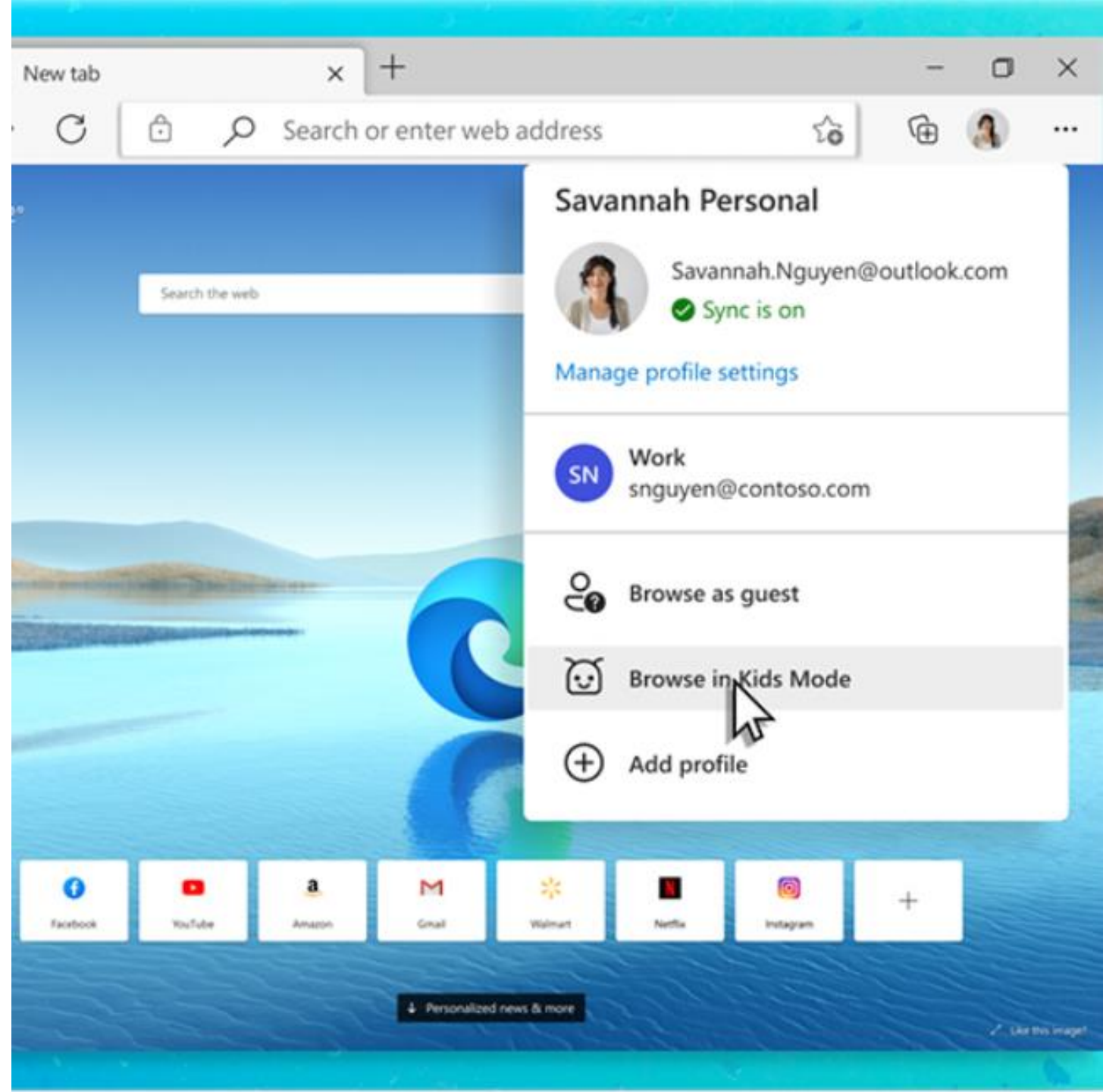
Microsoft Edge – Browse Safe with SmartScreen

Microsoft Defender SmartScreen helps you identify reported phishing and malware websites and also helps you make informed decisions about downloads

- ▶ As you browse the web, it analyzes pages and determines if they might be suspicious. SmartScreen checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites.
- ▶ SmartScreen checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe.

Safe browsing for kids with Microsoft Edge Kids mode

- ▶ Find Kids Mode in account options
- ▶ Choose their age group
- ▶ Easy for parents to switch modes



Secure your communication method

Use Web Content Filter

- ▶ Filters web traffic based off pre-configured policies set by the administrator.
- ▶ There are both home versions and corporate versions.
- ▶ Home versions focus on child safety, while corporate versions focus on employee productivity.
- ▶ Not only can it restrict the content that is displayed to a certain audience, it can also be utilized to filter malicious content and protect the user.

HTTPS

HTTPS Is a protocol for secure communication over a computer network which is widely used on the internet

No sensitive information should be typed into a page that is not secured by HTTPS.

Even though a page is secured with HTTPS, it does not automatically mean the page is safe.

Most browsers have begun to let users know more easily when they are on a non-secure page.



Secure

| <https://www.google.com>

Email Protection

Email Protection Overview



2FA



Password
Reset




Spam
Protection




Attachment
Policy


Two-factor authentication for Email



Email is most important account needing protection, because if someone gains access to your email, they can utilize the password reset function to gain access to other services



Most major email providers allow you to set up 2FA with your email account

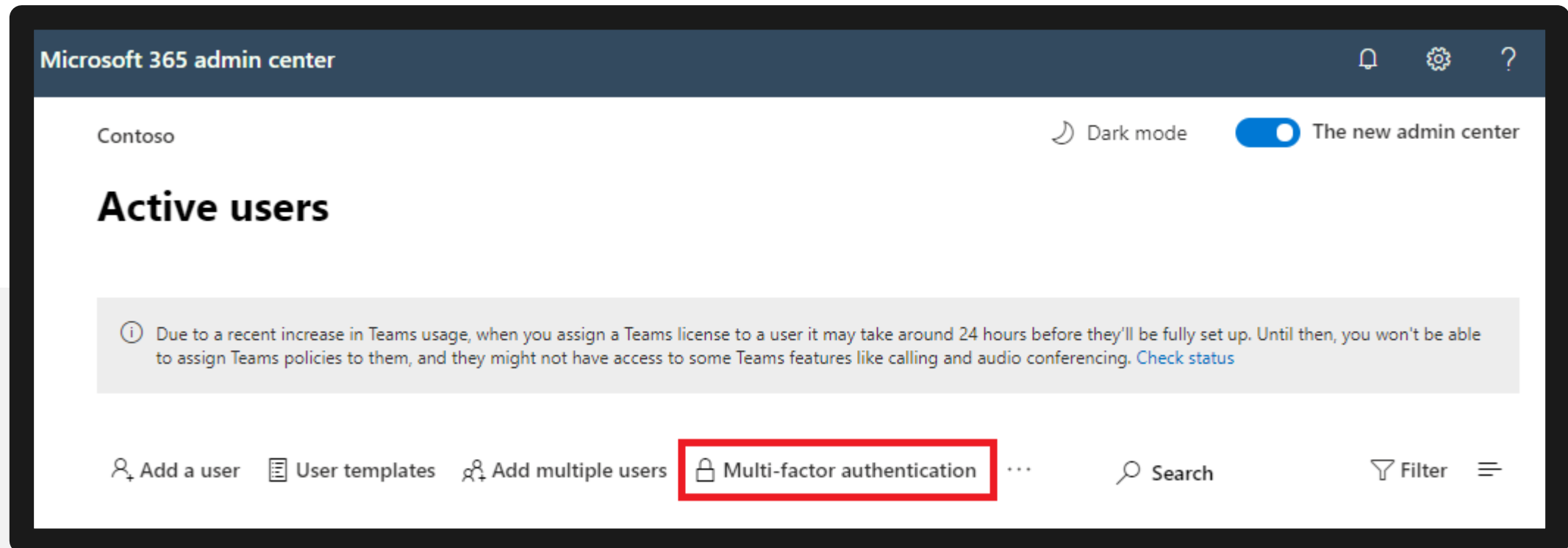


Once set up, the attacker would need your password and your cell phone in order to break into your email account

Multi-factor authentication for Microsoft 365

Azure AD Identity Protection

With Azure AD Identity Protection, you can create an additional Conditional Access policy to require MFA when sign-in risk is medium or high



Password Reset



When passwords are forgotten, the ability to reset your password is very convenient, but if not utilized properly this can allow someone to easily take over your account.

Some websites do not require any security questions to be answered or any additional information besides account email address to initiate a password reset.

Usually when someone requests a password reset, an email is sent to the email address on file with this information.

Monitor these emails and contact the vendor directly if you see these and did not initiate them yourself.

Spam Protection

- ▶ Everyone gets spam; even with the best protection, some still slips through the cracks.
- ▶ Some email providers have better spam protection than others.
- ▶ A third-party anti-spam product can supplement protection provided by the email provider.

Tips for Spam Protection



Never respond to spam emails

Be careful using your email address to sign up for contests or enter websites

When posting your email to a public website, always add special breaks in your email address.
Example: ben(at)eset dotcom

Use the security center to create anti-spam policies

Safe Attachment Policy

- ▶ Attachments are one of the most common ways to get viruses or malware
- ▶ Even though an attachment might look like a document or Excel file, it might contain a virus or malware
- ▶ Rules should be in place at your company to prevent receiving certain types of attachment files
- ▶ Employees should receive training that describes why attachments can be harmful
- ▶ Never open attachments from unknown senders
- ▶ If you see something that is questionable, send to your IT department for verification

Demo

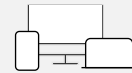
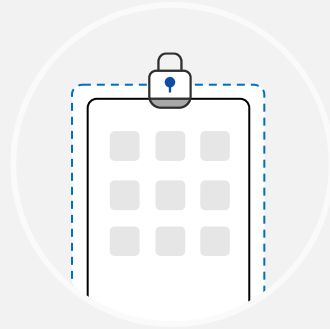
Creating Safe attachment policies with Microsoft Defender for Office 365

Protect your corporate data on your mobile devices

Mobile Device Management (MDM)

Conditional Access:

Restrict access to managed and compliant devices



Enroll devices for management



Provision settings, certs, profiles



Report & measure device compliance

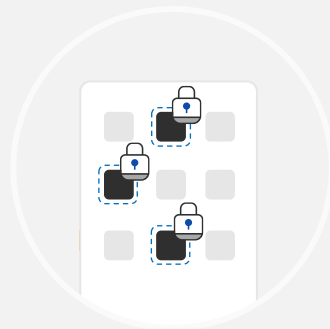


Remove corporate data from devices

Mobile Application Management (MAM)

Conditional Access:

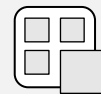
Restrict which apps can be used to access email or files



Publish mobile apps to users



Configure and update apps



Report app inventory & usage



Secure & remove corporate data within mobile apps

Corporate App Protection with Microsoft Intune

Familiar Office experience

- ▶ Seamless “enrollment” into app management
- ▶ Use for personal and corporate accounts

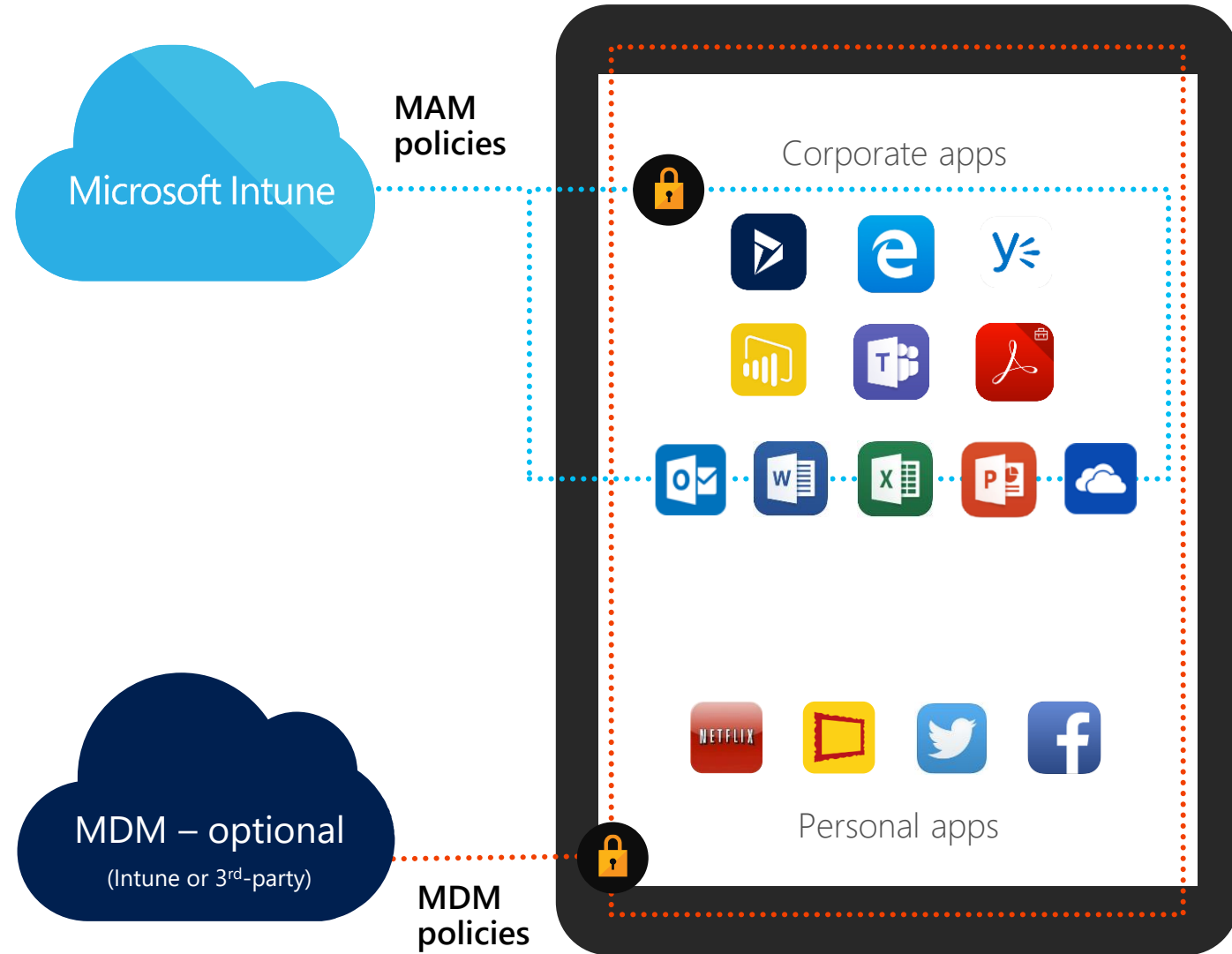
Comprehensive protection

- ▶ App encryption at rest
- ▶ App access control – PIN or credentials
- ▶ Save as/copy/paste restrictions
- ▶ App-level selective wipe

MDM mgmt. by Intune or third-party is optional

Might be a good solution for these scenarios:

- ▶ BYOD when MDM is not required
- ▶ Extending app access to vendors and partners
- ▶ Already have an existing MDM solution



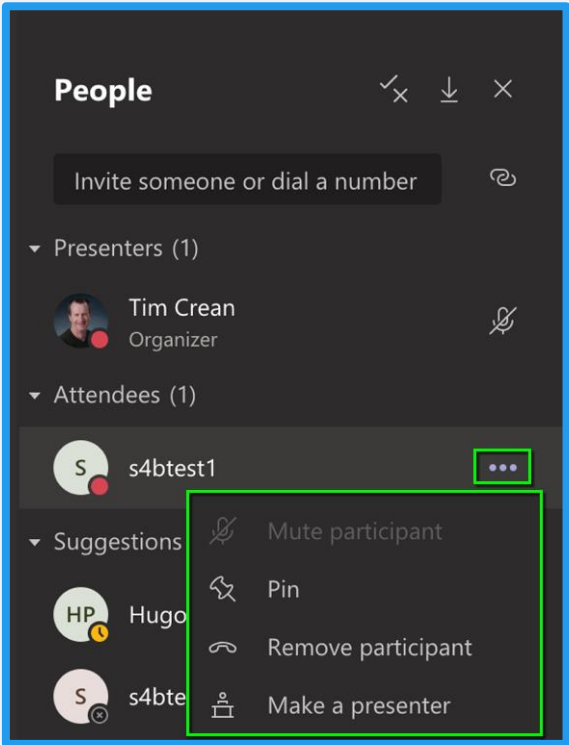
Threats to Students

Remote learning and technology integration in education have underscored the need for an in-depth understanding of how hackers can target students and steal their sensitive information

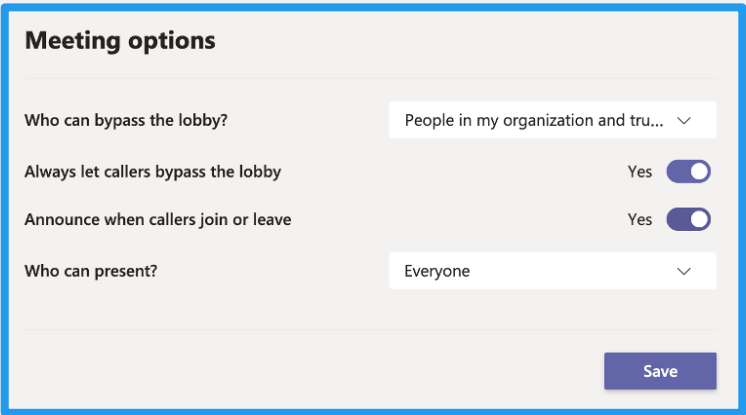
Ways Students can be targeted

- ▶ Phishing Messages
- ▶ Email Attachments on Links
- ▶ Video Conferencing Software
- ▶ Weak Passwords
- ▶ Physical Theft

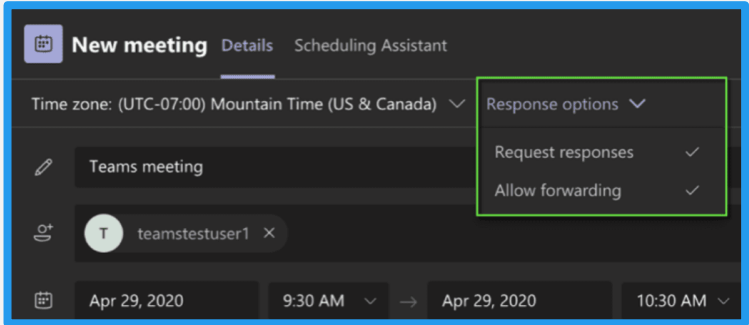
Securing meetings on Microsoft Teams



Ability to remove a participant



Choose meeting options while setting up a meeting



Choose response Options

Demo

Teams Meetings options

Preventive Measures

Preventive Measures



Define a clear attachment policy coupled with a spam filter.

Implement a Web content filter to help with malicious content, inappropriate content, and productivity issues.

Utilize unique passwords and maintain a clear password policy. If needed, use a password manager.

Keep all internet-connected devices up to date, including routers, IoT devices, computers, mobile devices.

Thank You

