PHISHING SECURITY

joe apps
TECHNOLOGY SUPPORT
joeapps.ca

Empowering communities through innovation, Delivering world class service and support.

Helping 5000 Innovative Businesses with Technology

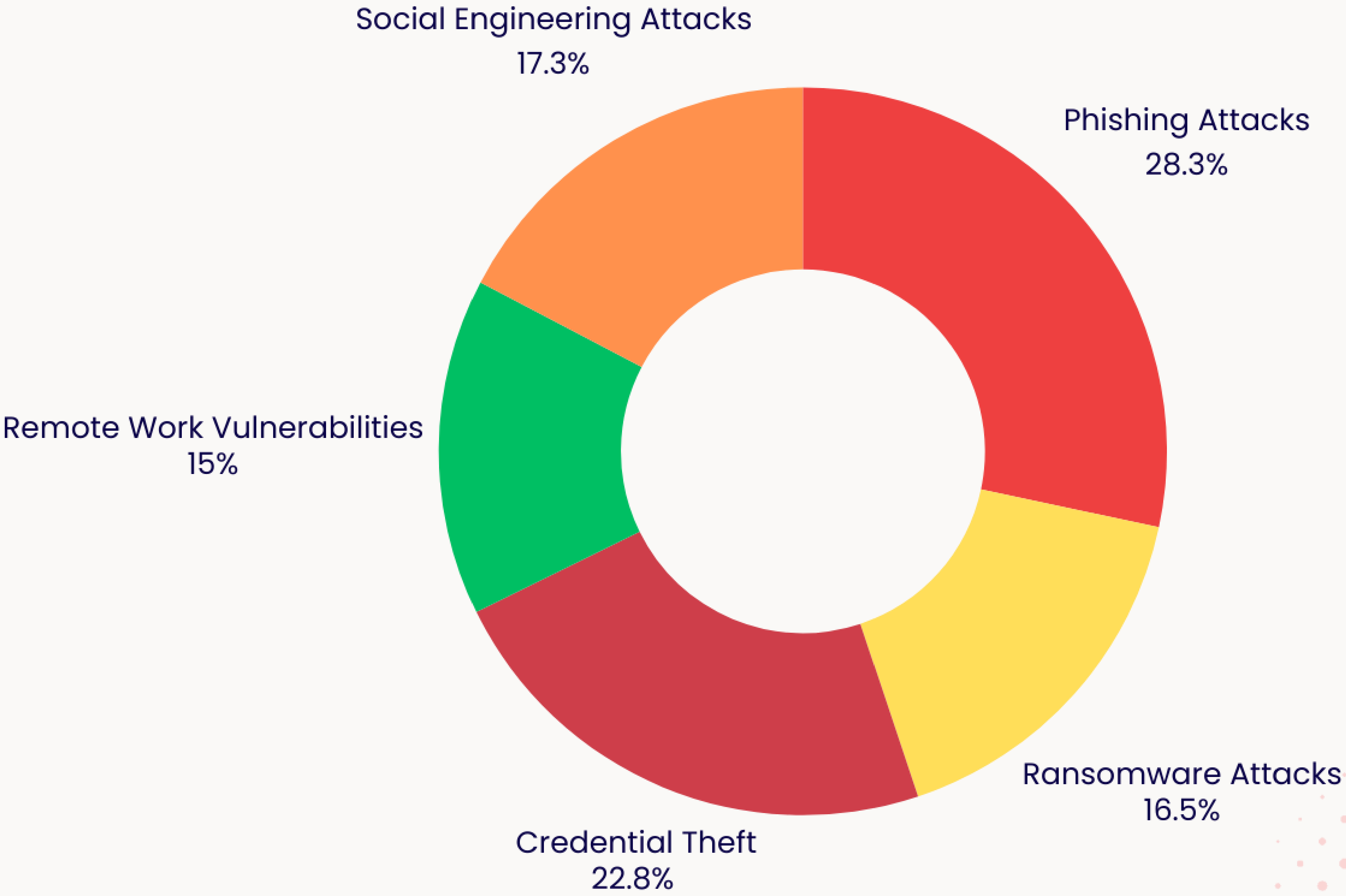
joe apps
TECHNOLOGY SUPPORT

INTRODUCTION TO PHISHING

Definition of phishing

Phishing is a cyberattack where attackers deceive users into providing sensitive information, such as passwords or credit card details, by pretending to be a trustworthy source, like a bank or a well-known company. These attacks often come through fake emails, messages, or websites that look legitimate. By recognizing suspicious links and verifying the source before sharing information, users can protect themselves from falling victim to phishing scams.

RECENT CYBERSECURITY TRENDS AND WHAT YOU NEED TO KNOW (2024)



TYPES OF PHISHING

Email Phishing

Description: The most common form, where attackers send fraudulent emails that appear to be from reputable sources (banks, service providers, etc.).

How it works: The email includes a link or attachment that, when clicked, installs malware or leads to a fake login page designed to steal credentials.

Example: An email that looks like it's from your bank asking you to verify your account by clicking a link.

joe apps
TECHNOLOGY SUPPORT

TYPES OF PHISHING

Spear Phishing

Description: A targeted attack aimed at a specific individual or organization, often using personal information to make the email more convincing.

How it works: The attacker usually gathers information on the victim from social media or corporate websites to tailor the email.

Example: An email to an employee from what looks like their boss, asking for sensitive company information.

TYPES OF PHISHING

Whaling

Description: A highly targeted form of phishing aimed at senior executives or high-profile individuals in an organization.
How it works: Attackers mimic communication from a trusted source like a business partner or a fellow executive.
Example: An email from what appears to be the CEO asking for a wire transfer for a "critical business deal."

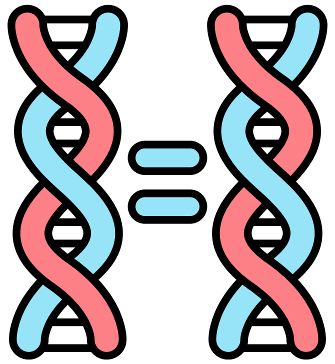
TYPES OF PHISHING

Clone Phishing

Description: Attackers copy a legitimate email previously sent to the victim but replace the attachment or link with a malicious one.

How it works: They resend the email with a message like, "Here is the document you requested."

Example: Re-sending a company-wide memo with an altered link to a malicious site.



TYPES OF PHISHING

Vishing (Voice Phishing)

Description: Phishing attempts that happen over the phone or voicemail.
How it works: The scammer calls pretending to be from a trusted organization, such as your bank, and asks for personal details or financial information.
Example: A call from "tech support" claiming your computer has a virus and asking for remote access.

TYPES OF PHISHING

Smishing (SMS Phishing)

Description: Phishing via text message or SMS, where scammers trick recipients into clicking on a malicious link or providing personal details.

How it works: Victims receive a message that appears to be from a trusted service, often with urgent language to prompt immediate action.

Example: A text from a delivery service asking you to click on a link to reschedule a package.

SMS

EMAIL SOLICITATION SCAMS

What is an Email Solicitation Scam?

Definition: Email solicitation scams involve unsolicited emails from scammers claiming to offer goods or services, often targeting specific groups or businesses.

Chamber of Commerce Target: Scammers often target member directories, offering these lists for sale to unsuspecting buyers or claiming to provide marketing services using the directory information.

SCAM SCAM! SCAM

joe apps
TECHNOLOGY SUPPORT
joeapps.ca

WAYS TO HELP YOURSELF!

Help to prevent phishing attacks

FIRST STEPS TO PREVENT AN ATTACK

Enable Multifactor Authentication (MFA)

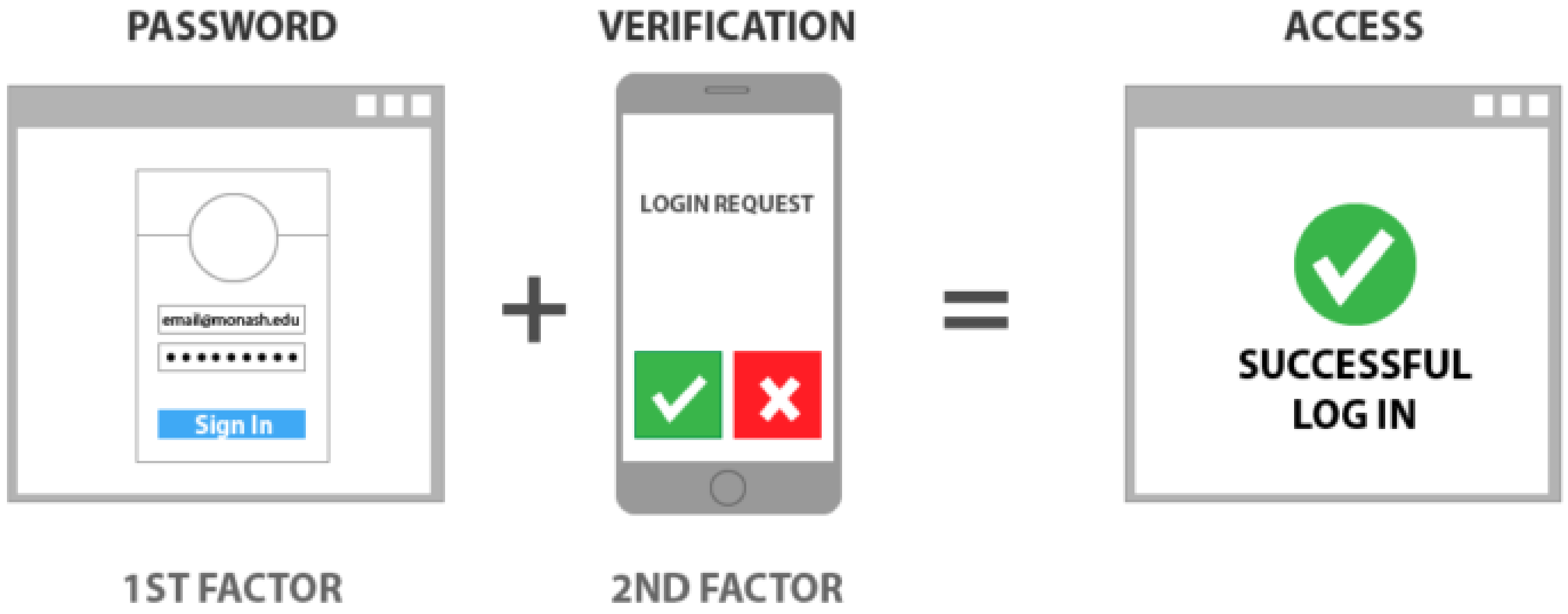
Why: MFA adds an extra layer of security by requiring more than just a password to access accounts.

How: Set up MFA on all critical accounts, using an authentication app or SMS codes to verify your identity.

Regularly Update Software and Devices

Why: Updates often include security patches that fix vulnerabilities exploited by cyber attackers.

How: Enable automatic updates on your devices and applications, including your operating system, antivirus software, and web browsers.



joe apps
TECHNOLOGY SUPPORT

NEXT STEPS TO PREVENT AN ATTACK

Use Strong, Unique Passwords and a Password Manager

Why: Strong passwords make it harder for attackers to gain access through credential theft or brute force attacks.

How: Create complex passwords for each account and store them securely using a password manager, which can generate and remember strong passwords for you.

Be Cautious with Emails and Links (Avoid Phishing)

Why: Phishing attacks are a common method to trick users into revealing sensitive information or downloading malware.

How: Verify the sender's email address, avoid clicking on suspicious links, and never provide personal information unless you are certain of the source. Hover over links to check their destination before clicking.

PROTECT YOURSELF

Backup:

Keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite or in the cloud.

We have a saying here about backups, There are two types of people those, who back up and those who are yet to lose their data.

Use these helpful resources to stay alert:

Website: haveibeenpwned.com, Check to see if your information is available on the dark web

Website: mxtoolbox.com/, Check to see your email records.

Website: joeapps.ca/blog, Check to see up-to-date Cyber Security information and technology trends each month!

EMERGING TRENDS IN CYBERSECURITY

Email impersonation is a tactic used by attackers to send emails that appear to come from a trusted source. It's commonly used in phishing attacks to trick recipients into sharing sensitive information or clicking malicious links.

Email Verification

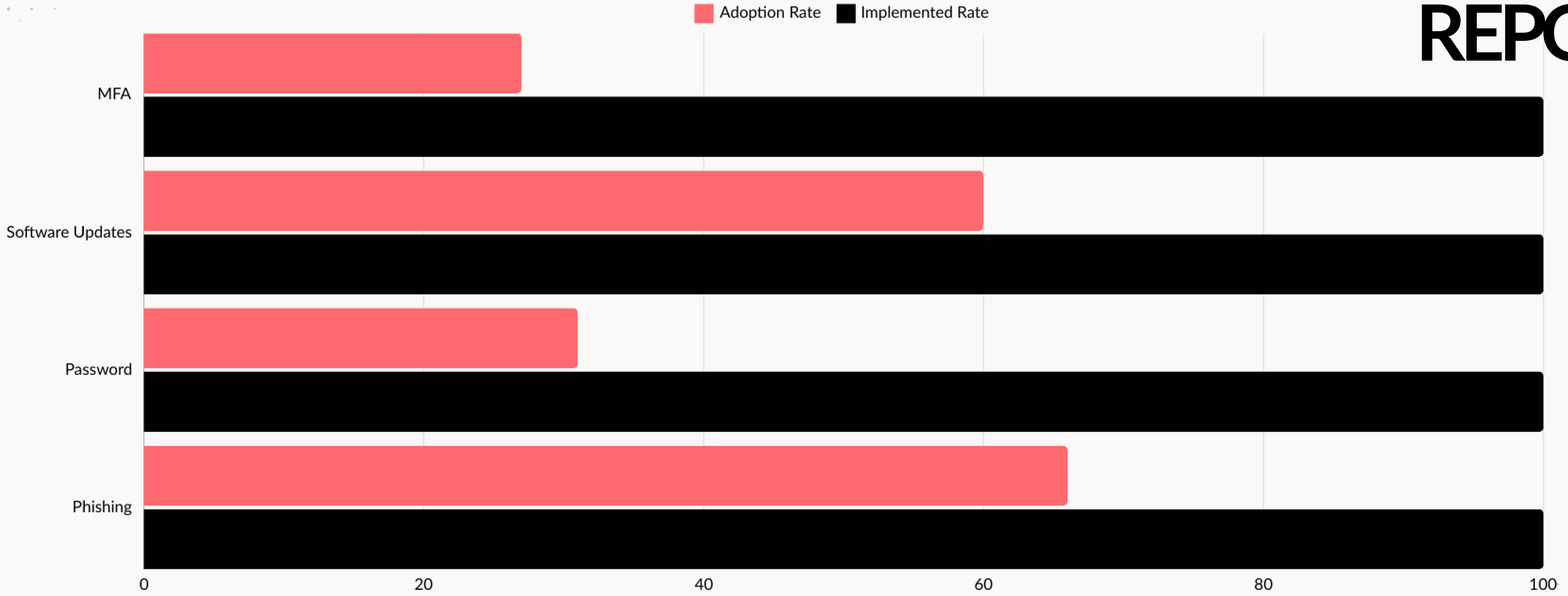
DKIM Records: Adds a digital signature to emails, which can be verified by the recipient's mail server to ensure authenticity.

SPF (Sender Policy Framework): Specifies which IP addresses are allowed to send emails on behalf of your domain.

DMARC (Domain-based Message Authentication, Reporting, and Conformance): Works with DKIM and SPF to specify how to handle emails that fail authentication checks.

joe apps
TECHNOLOGY SUPPORT

CYBERSECURITY ADOPTION RATE REPORT



joe apps
TECHNOLOGY SUPPORT

joeapps.ca

Q+A

joe apps

TECHNOLOGY SUPPORT

joeapps.ca

THANK YOU FOR YOUR TIME!

CONTACT US FOR A FREE CYBER ASSESEMENT

Don’t Go Alone, Get a Joe Today!