LastPass •••|

Combatting Social Engineering in 2024

From Adaptation to Elimination

Just as we have evolved, so too have the threats that prey upon the things that make us human.

Psychological manipulation through social engineering will continue to be a pervasive threat to businesses and their employees in 2024.

Employees are the first line of defense in safeguarding a company's sensitive data, yet they are also its weakest link, and can be easily manipulated by bad actors seeking sensitive data and credentials.

The first step in combating social engineering is to recognize the problem and its prevalence.

We surveyed **1,000 SMB and mid-market IT professionals** from the **United States, United Kingdom, France, Germany,** and **Australia** to gauge how social engineering has affected their organizations and what they're doing to defend against this threat.

The results?

- Businesses need to **adapt** to the evolutionary nature of social engineering.
- There is **cognitive dissonance** with the efficacy of their current defenses.
- Businesses want to **eliminate** the crux of these attacks: **passwords.**

What is social engineering?

Social engineering attacks manipulate people into sharing information they shouldn't or making other mistakes that compromise their personal or organizational security (Source: IBM).

Phishing will continue to be the biggest threat to businesses, made even more harmful with Gen AI

Phishing has increased the most over the past year for businesses, **far exceeding business email compromise, vishing, smishing, and baiting.**

81% **of businesses have seen an increase in phishing this past year.**

Phishing is also forecasted as the biggest social engineering threat to businesses in 2024.

Understanding types of social engineering

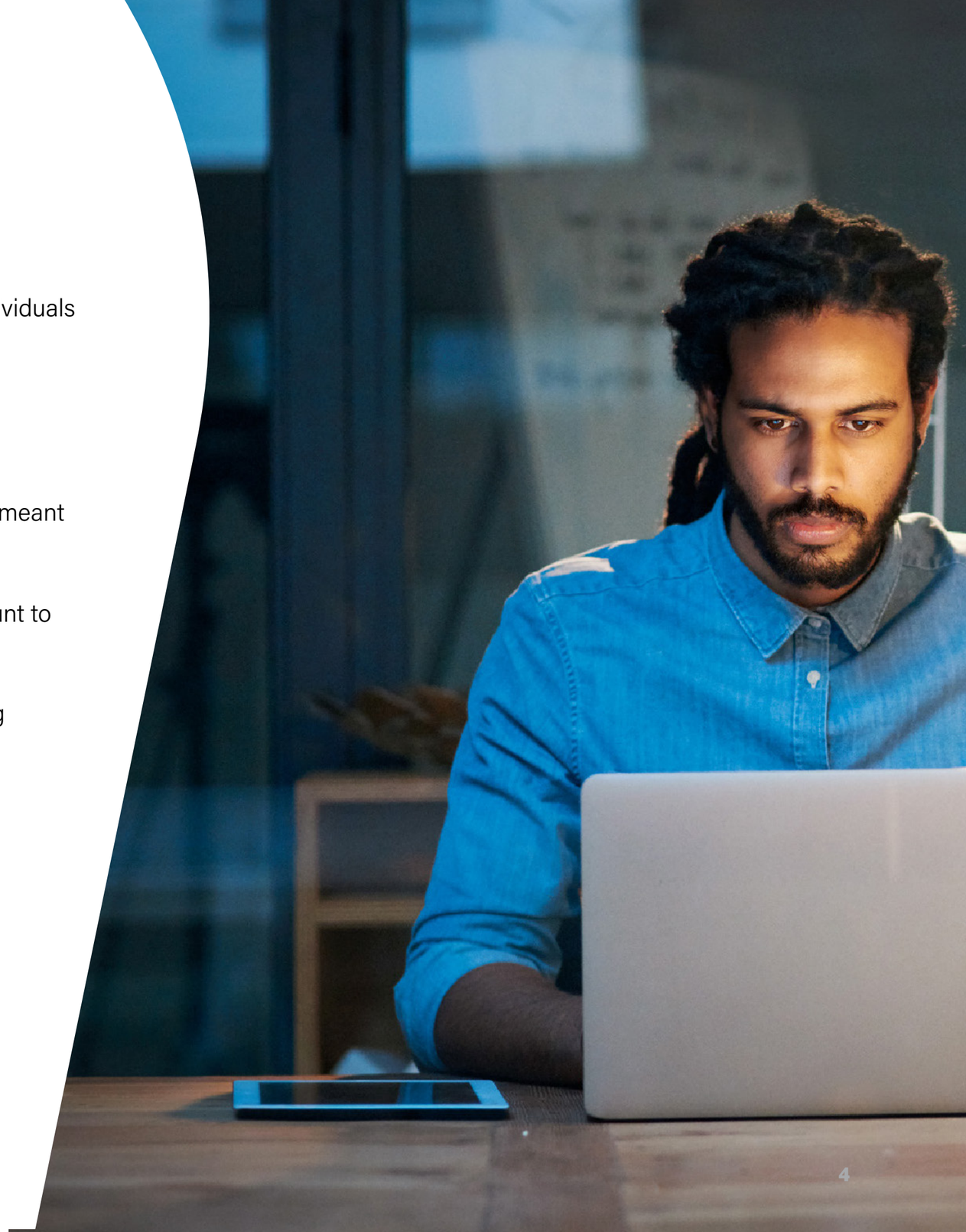
Phishing: Emails purporting to be from reputable companies to induce individuals to reveal personal information or sensitive data.

Vishing: Fraudulent phone calls that induce individuals to reveal personal information or sensitive data.

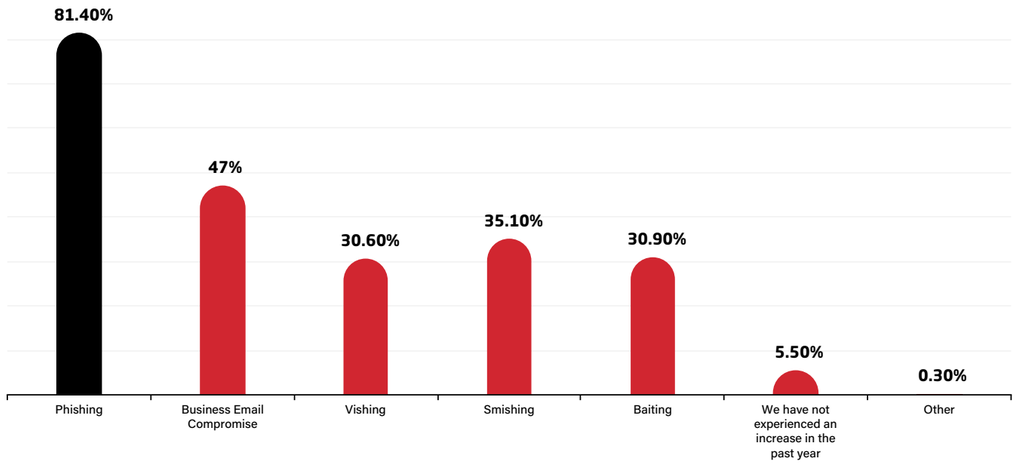
Smishing: Text messages (SMS) purporting to be from a reputable source meant to trick the recipient into revealing personal information or sensitive data.

Business email compromise: Obtaining access to a business email account to imitate the owner's identity.

Baiting: A scammer uses a false promise to lure an individual into revealing personal information or sensitive data.



Within your organization, what types of social engineering have you seen increase this past year?



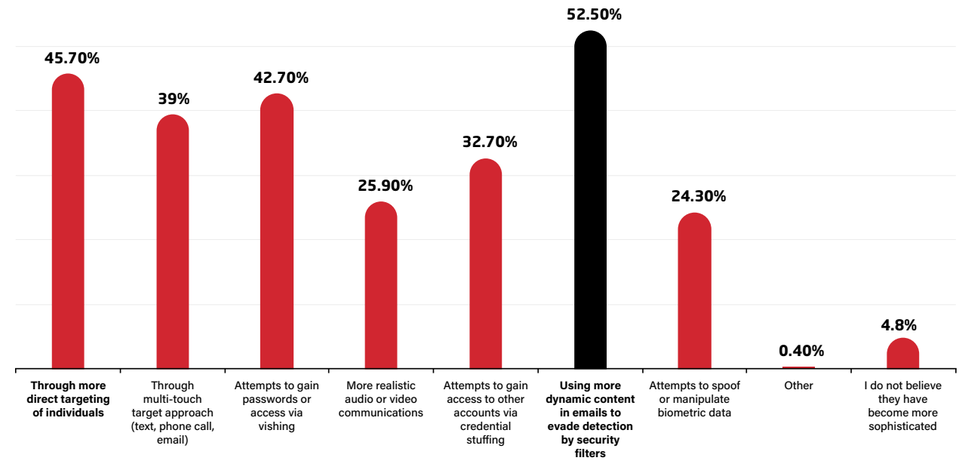
Dynamic content (a/k/a adaptive content) in emails through Gen AI is making detecting phishing attempts harder. Gone are the days of a misspelled word or bad grammar alerting an employee to a potential phishing attack.

What is Gen AI? Gen AI or Large Language Models (LLMs) are foundational models trained on immense amounts of data making them capable of understanding and generating natural language. This dynamic content can be tailored to the individual recipient and includes natural-sounding email copy. (Source: IBM).

52.5% **report that social engineering attacks are using more dynamic content in emails influenced by Gen AI making phishing harder to identify.**

45.7% **report that social engineering attacks are increasing direct targeting of individuals.**

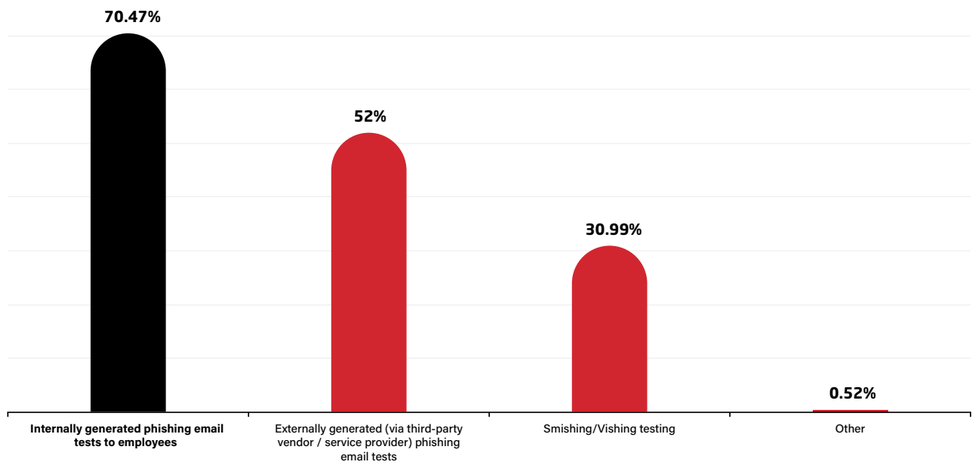
Within your organization, how have social engineering attacks become more sophisticated over the last year?



95% **have seen social engineering attacks become more sophisticated in general.**

As a result, organizations are seeking **bespoke programs created in-house** to adapt and combat the personalized nature of phishing attacks using Gen AI.

What does your company's phishing testing program consist of?



How to avoid phishing emails in the Gen AI era:

- Verify messages from people you know.
- Be careful with MFA prompts you don't recognize.
- Don't click on any attachments or links without verifying the sender.
- Be wary of urgent language.

But are these programs really working?

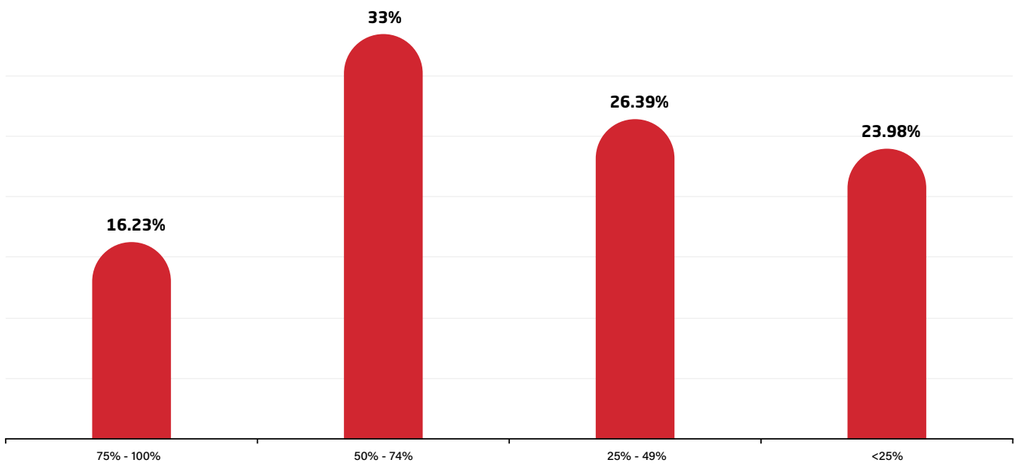
Cognitive dissonance is high when it comes to the efficacy of phishing testing programs

There is a high vote of confidence from respondents when it comes to their organization's phishing testing programs.

88% **of respondents think that their company's phishing testing program is effective.**

But does perception match reality when it comes to the efficacy of these programs?

How many users are reporting suspicious activity within the phishing testing program?



Only 16% of users report 75-100% of suspicious activity within their phishing testing program.

This clear cognitive dissonance means that simply ticking the boxes when it comes to implementing a phishing testing program could leave your business susceptible to attacks.

As social engineering becomes more sophisticated, employees and employers must be active participants in the fight against phishing attempts. To combat the evolving nature of these attacks, they must be vigilant -- and as adaptable as the threat itself.

Phishing testing program pro tips:

Set measurable, attainable KPIs to track improvement over time

Establish a consistent cadence of testing to keep employees alert and engaged

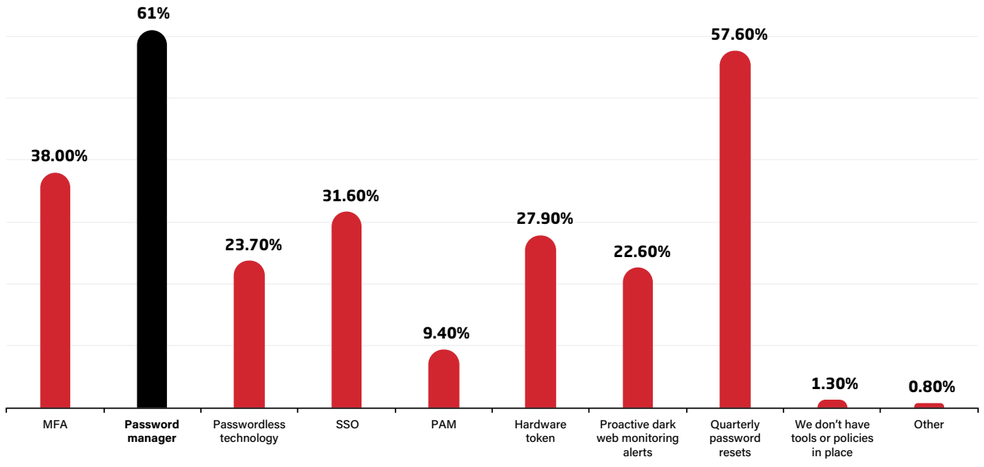
Continue to educate on phishing tactics (like the use of Gen AI) on a regular basis

How can an organization truly safeguard itself from this evolving threat landscape?

Password managers are key to combatting social engineering

61% **of respondents use a password manager to prevent user credentials from being exposed via social engineering, more than MFA, SSO, and PAM.**

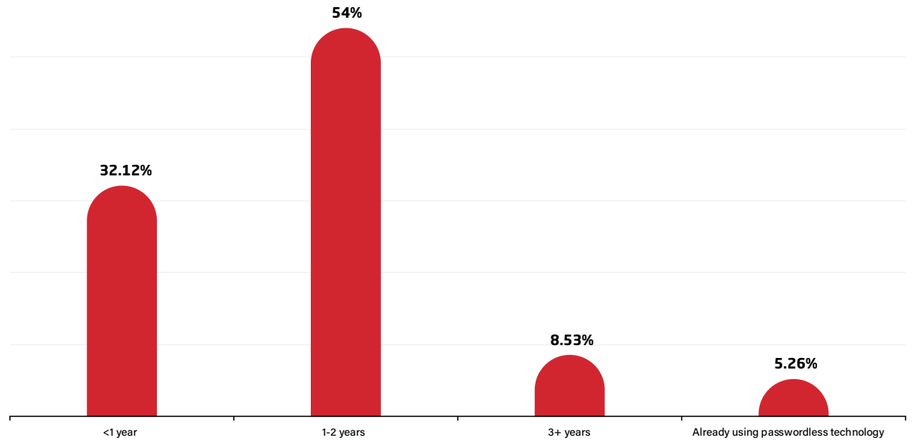
What protections (tools / policy) do you have in place to prevent user credentials from being exposed via social engineering? Select all that apply.



However, passwords are vulnerable and dependent upon the behavior of your employees. The solution? Fewer passwords, a/k/a password[less].

86% **of organizations plan to reducepasswords in two years or less.**

What is your timeline to reduce passwords?



The adoption of passkeys will be a crucial step in the eradication of social engineering attacks. When you remove the password, you eliminate the phishable key to your company's data.

78% **of organizations agree that the removal of passwords through passkeys will eventually help reduce the threat of social engineering.**

Adapting to the evolving nature of social engineering attacks, particularly phishing, is crucial to the integrity and safety of your business's data.

Ultimately, though, the elimination of passwords will be the strongest defense against a type of attack that manipulates human fallibility.

Social engineering will have to contend with a password[less] future just as we must embrace a digital life with fewer credentials.

Prepare for a password[less] future by embracing pervasive password management today with LastPass.

With a password manager you can reduce your organization's use of passwords and reliance on human behavior.

- **Manage passwords from one place**
- **Protect your sensitive data from one hub.**
- **Share passwords simply and safely**
- **Go passwordless – as you're ready for it**

LastPass •••|

With over 1 billion sites secured, millions of users, and 100,000 Business customers, LastPass makes online security simple.

Contact us