BUSTING MYTHS:
MAINFRAME PHISHING ATTACKS

1

MYTH
Mainframes are 100% secure.

REALITY
Mainframes are still vulnerable to breaches from phishing attacks.

MYTH
Mainframes encrypt data, protecting against all attacks.
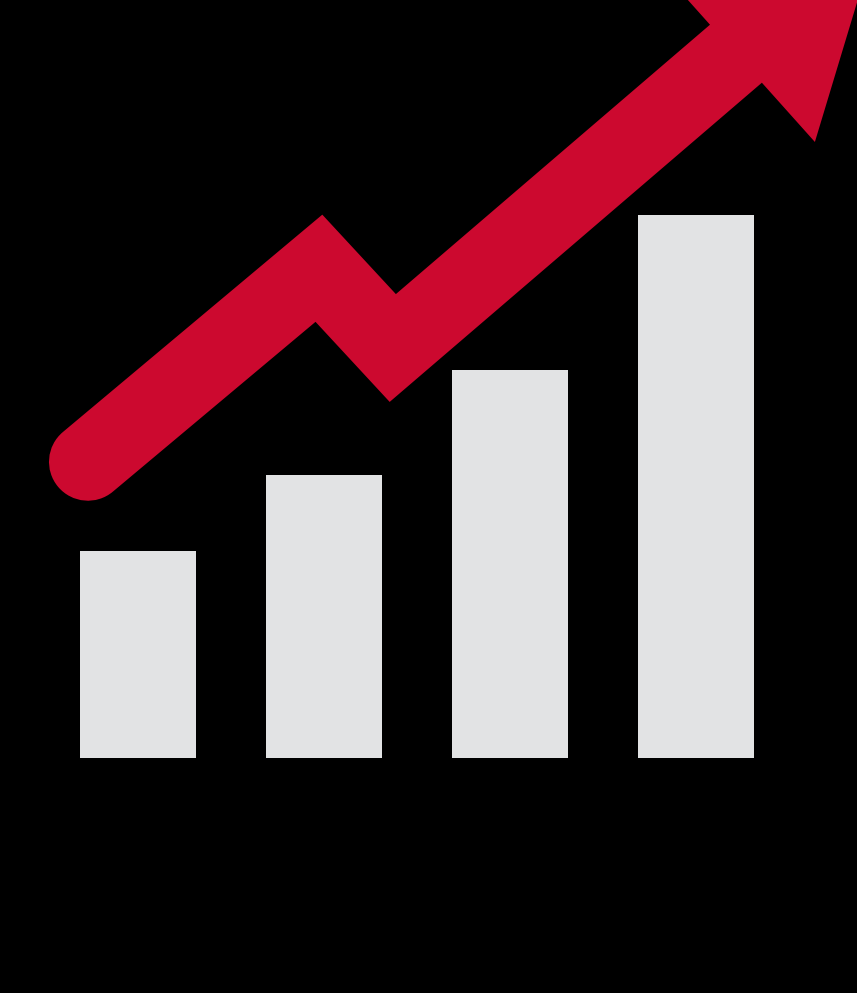
REALITY
Mainframes are often overlooked due to inaccurate assumptions, complexity and a lack of trained expertise.

MYTH
Mainframe phishing attacks are rare.

REALITY
Phishing is the most common way for criminals to access corporate networks. Up to 90% of breaches start with phishing.

33%
Over 33% of attacks X-Force remediated in 2021 involved phishing

Source: IBM Security X-Force Threat Intelligence Report
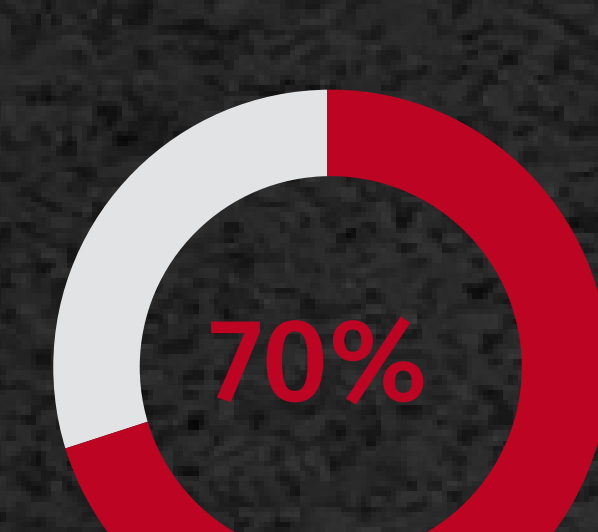
MYTH
Damages are not that severe.

REALITY
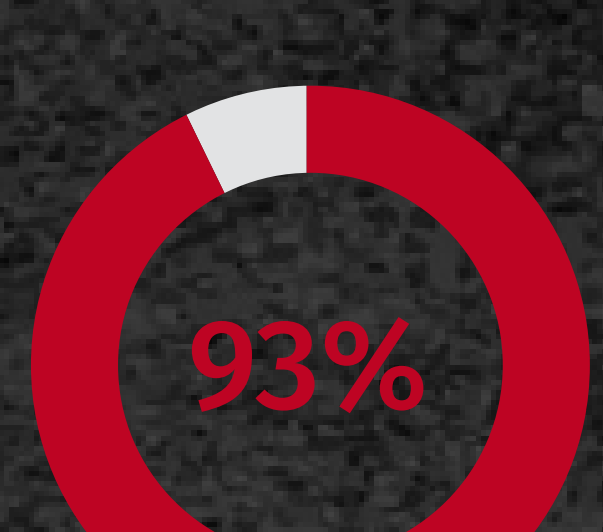Data breaches stemming from phishing cost companies an average of **$4.65 million** in 2021.

Don't fall into the trap of believing your mainframe is safe from a phishing attack.

- Mainframes are not bulletproof.
- Mainframes almost always hold your most valuable organizational assets.
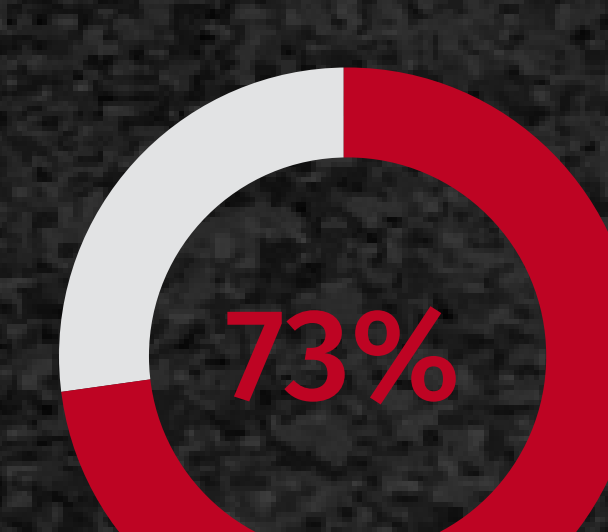- Phishing attacks can compromise mainframe credentials.

Mainframes...

70% Run 70% of the world's mission-critical applications

93% Perform financial management for 93% of companies

73% Complete approximately 73% of customer transactions

Source: IBM IBM and Forrester sponsored by Broadcom

Take action today.

Identify risks. Control access rights. Assess data encryption. Monitor critical resources. Broadcom mainframe customers are entitled to phishing protection tools and our experts stand ready to help with deployment. Don't delay – contact us today.

To build resilience and mitigate the risks of cyberattacks such as phishing, it's important to follow these best practices for safeguarding your mainframe.

Explore More Resources