Optimize your cyber insurance strategy

Reduce risk and cost with phishing-resistant MFA

Cyber attacks, such as phishing and ransomware, are getting more pervasive, sophisticated, and expensive by the day, leading to higher cyber insurance premiums and stricter underwriting requirements. Qualifying for cyber insurance is a vital risk management strategy that businesses can't afford to ignore.

New Standards Implementing strategies to prevent cyber attacks before they happen are essential, which is why cyber insurance providers are increasingly requiring that multi-factor authentication (MFA) be in place prior to writing new policies.

The cyber insurance landscape is quickly changing

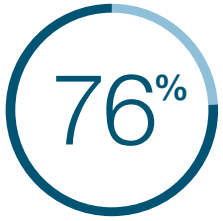
The spike in security breaches, caused by phishing and ransomware, have led to massive payouts to malicious actors. Stolen credentials are at the root of 80% of breaches.

Organizations looking to qualify for cyber insurance need to adopt not just any MFA, but phishing-resistant MFA to stop account takeovers and ransomware in their tracks.

Businesses that reconsidered partnerships without comprehensive cyber insurance

Companies with cyber insurance coverage have used it—and 50% have used it more than once

Small to medium-sized enterprises with no cyber insurance would be heavily impacted by an attack



Phishing-related cyber insurance claims filed in 2022

The average cost of a ransomware attack in 2022—excluding the ransom itself

yubico

Phishing-resistant MFA is your compass to navigate today's cyber insurance landscape

Cyber insurance isn't a golden ticket to peace of mind, nor should it be your only proactive line of defense. According to the U.S. Government Accountability Office, cyber insurance is limited in its ability to cover potentially catastrophic losses from systemic cyberattacks.

You need a strategy to prevent cyber attacks before they happen, which is why cyber insurance providers are increasingly requiring that multi-factor authentication (MFA) be in place before they write new policies.

Not all MFA is created equal

Most traditional MFA methods are insecure. Legacy MFA such as SMS, one time passwords, and even mobile push authenticators are susceptible to account takeover attacks from phishing and man-in-the-middle attacks.

Organizations need modern MFA that involves either Smart card/PIV or modern FIDO authentication. Hardware security keys based on these methods can stop account takeovers in their tracks and prevent ransomware and other modern threat vectors.

Sources: Forbes, Delinea, Security Magazine, IBM, Coalition

Read our **cyber insurance whitepaper.**
Learn how to better qualify for cyber insurance.

YubiKeys are a future-proofed security investment that reduces risk and costs

Phishing-resistant MFA makes it easier to qualify for cyber insurance and, in some cases, cheaper. Just ask Afni, which saved 30% on its premiums by using YubiKeys:

YubiKey 5C NFC

"When I'm going down by a third and others are going up by 20% or higher, that's a really big win."

Brent Deterding, AFNI CISO

yubico