December 11, 2024

To whom it may concern:

We appreciate the opportunity to provide comments to ENISA on the draft Implementing Guidance for NIS2 Security Measures.

As background, the Fast Identity Online (FIDO) Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, telecommunications, and fintech, as well as those in security, health care, and information technology.


The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the twelve years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like one-time passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today, the FIDO standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy authentication tools. They are supported by a broad ecosystem of more than 1000 products that have been certified as meeting the FIDO standards, ensuring that enterprises of all sizes are able to choose from a variety of interoperable, standards-based products to meet their authentication needs. Moreover, with the FIDO Web Authentication protocol being a W3C standard, ever major browser and platform ships with

native support for FIDO, making phishing resistant authentication as easy (or often easier) to deploy as legacy authentication tools.

However, as we detail in our comments below, we are concerned that the draft implementing act for NIS2 does not sufficiently differentiate between phishing-resistant authentication and legacy authentication tools that are increasingly vulnerable to phishing attacks.

**The importance of phishing-resistant authentication – and FIDO standards – is recognized across the globe.**

- ENISA and CERT-EU highlighted the importance of FIDO in a 2022 publication entitled "Boosting Your Organization's Cyber Resilience (JP-22-01),"[1] noting:

  > *"If possible, avoid using SMS and voice calls to provide one-time codes and consider deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys."*

- The Netherlands National Cyber Security Center (NCSC) highlighted the importance of phishing-resistant authentication in its publication "Mature Authentication – Use of Secure Authentication Tools."[2] That guidance notes:

  > "A distinction can be made between the implementation of two-factor authentication (2FA) and phishing-resistant authentication" and goes on to note that SMS, software tokens and hardware tokens are all *"not totally resistant to phishing."*
  >
  > It goes on to advise that *"A standard from the FIDO Alliance, known as FIDO2, is resistant to phishing. Therefore, tokens that implement this standard provide the most comprehensive protection for authentication at this time."*

- In the US, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory[3] echoing the concerns of ENISA and the NCSC, noting:

  > *"Not all forms of MFA are equally secure. Some forms are vulnerable to phishing, "push bombing" attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM Swap attacks. These attacks, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems."*

  The CISA guidance goes on to note:

  > *"While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort,"* and also notes that *"The only widely available phishing-*

[1] See https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

[2] See https://english.ncsc.nl/publications/factsheets/2022/juni/9/factsheet-mature-authentication---use-of-secure-authentication-tools

[3] See https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching

*resistant authentication is FIDO/WebAuthn authentication."* – although it notes that PKI-based MFA is also phishing-resistant, if not as widely available.

- Also in the US, an August 11, 2022 circular[4] from the U.S. Consumer Financial Protection Bureau (CFPB) states:

  *"MFA solutions that protect against credential phishing, such as those using the (FIDO) Web Authentication standard supported by web browsers, are especially important."*

- We also note that a 2023 Cyber Safety Review Board (CSRB) report[5] of the attacks associated with the LAPSUS$ Group stated:

  *"In the past decade, the emphasis on MFA has driven the adoption of more secure solutions to improve resiliency against attacks and phishing in particular. Enterprise and consumer adoption of MFA has been a beneficial step forward away from use of just passwords for authentication. However, the Board's review found that the types of MFA used broadly in the online ecosystem today are not sufficient for most organizations or consumers defending against the type of attacks described in this report.*

  *"In particular, OTP delivery and push notifications using SMS and voice calls (and even email) are vulnerable to social engineering and SIM swap attacks, and the attacker ecosystem is readily capable of exploiting these weaknesses. A lucrative SIM swap criminal market is enabling pay-for-access to victim mobile phone services with a focus on hijacking SMS messages and voice calls. SMS was not designed to transact sensitive information such as OTPs, and its wide use as such incentivizes criminals to perform SIM swap attacks, porting fraud, and similar techniques.*

  *"Web and mobile application developers should leverage Fast IDentity Online (FIDO)2-compliant, hardware-backed solutions built into consumer devices by default. Use of these built-in tokens should have easy integration with applications and web-based services, leveraging standards such as WebAuthn and technologies such as Passkeys".*

**Concerns with the draft implementing guidance**

Against this backdrop, we wanted to flag our concerns that the draft implementing guidance is silent when it comes to acknowledging the concerns that ENISA and other agencies have flagged about legacy authentication tools. It would seem that the draft should echo these points, and note that legacy authentication tools are increasingly vulnerable to phishing attacks and encourage implementers to select authentication technology that can stand up against these attacks.

We believe these points should be communicated in both Section 11.6 (Authentication) and Section 11.7

[4] https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

[5] https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

(Multi-Factor Authentication).

**Section 11.6 (Authentication)**
While this section deals mostly with passwords, it does list a number of "common authentication technologies" but does not include FIDO. We suggest that the list be amended to include the following:

- Passkeys: Discoverable FIDO credentials that enable passwordless, phishing-resistant authentication.
- FIDO2 Security Keys

While our comments here are primarily concerned with the recognition of FIDO authenticators, we also believe it would make sense to list smart cards here, much as ENISA did in its 2022 publication referenced on the previous page. The reason is that authentication based on smart cards is usually phishing-resistant as well.

We also note that OAuth is listed but is not generally viewed as an authentication standard; instead it deals with authorization. OpenID Connect is the authentication standard which builds on top of OAuth 2.0 to deliver authentication, and would be more appropriate to list here.

**Section 11.7 (Multi-Factor Authentication)**
Here, we believe a more detailed discussion of the vulnerabilities of legacy MFA tools to phishing is needed to better help implementers understand the risks associated with different types of MFA, similar to what ENISA flagged in its 2022 guidance with CERT-EU, or what NCSC, CISA, and the CSRB have noted. While we understand that ENISA may not wish to be overly specific, the draft does dive into many other specific details around MFA implementation, such as integrating MFA with SSO and monitoring MFA logs for suspicious activity.

Here we would recommend a number of edits to address this issue and ensure that implementers are aware of the difference between legacy MFA and phishing-resistant MFA:

- In Section 11.7.1, we recommend:
  - Adding a sentence to the original statement on "relevant entities" to note: *"Some types of MFA are vulnerable to phishing attacks, and relevant entities should select MFA that can stand up to these attacks."*
  - Under the list of MFA methods listed under "Guidance," add:
    - Passkeys: Discoverable FIDO credentials that enable passwordless, phishing-resistant authentication.
    - FIDO2 Security Keys
    - Smart Cards
  - Under "Examples of Evidences," amend the second bullet to read: "Access control policy outlining how different MFA methods are assigned, *including whether phishing-resistant MFA is used."*

- In Section 11.7.2, we recommend adding a bullet to the "Guidance" heading that reads: *"Wherever possible, use phishing-resistant MFA such as FIDO2 security keys, passkeys, or smart cards to guard*

*against legacy MFA tools such as SMS, OTP, and Push Notifications that are vulnerable to phishing attacks."*

- In the "Tips" section, we recommend adding a bullet that reads: *"Some forms of legacy MFA such as SMS, OTP, and Push Notifications are now vulnerable to phishing attacks. Wherever possible, use phishing-resistant MFA such as FIDO2 security keys, passkeys, or smart cards, which can block these attacks."*

These minor changes would be quite effective in highlighting the threat of authentication being phished, and would help to prompt implementers to leverage phishing-resistant authentication wherever possible.

We greatly appreciate ENISA's consideration of our comments. We look forward to further discussion with the Commission on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this letter.

Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should ENISA officials wish to learn more about how FIDO authentication and how its certification programs work.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.