


A grayscale image of a hand reaching down from the top left corner of the slide.

A Matter Of Trust: When Security Is Not Enough

Michael Markevich
Security Advisor, CISO

A grayscale image of a hand reaching up from the bottom left corner of the slide.

Who Am I

- CISO at Gateway.fm, ex-CISO at Opera (Nasdaq:OPRA)
- Security lead for the DHI2 project
- Startup advisor and academic lecturer
- Sysadmin, penetration tester, IT auditor, amateur developer



A Minute For Stories

How do you select software and services?



Question Time

What software do you trust?

Sources Of Trust

- Knowledge
- Recommendations
- What else?

Definition Of Trust

Assured reliance on the character, ability, strength, or truth of someone or something.

/ The Merriam-Webster Dictionary /

Uncertainty And Trust

Assured means characterized by certainty or security.

Trust reduces uncertainty and increases the feeling of security.

Feeling Of Security?

"Security is both a feeling and a reality, and they're different." (Bruce Schneier)

Typical Situations

- Vendor (startup) - Client (big company)

Or vice versa:

- Vendor (Big company) - Client (startup)

My Software Trust Checklist

- Developed in the corporate times when evaluating vendors
- Strengthened during the startup times when looking for clients

Checklist /01

Is a "Security" page present on a website?

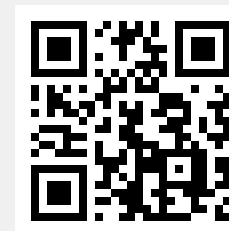
A good example: Obsidian's Security Page (<https://obsidian.md/security>)



Checklist /02

Does the company disclose their security contacts?

A good example is using *security.txt* file.



Checklist /03

Does the company have a vulnerability policy?

Checklist /04

Does the company run a bug bounty program?

Checklist /05

Does the company's product have a public threat model?



Checklist /06

Does the company have a technical blog or social media presence? Is the content written by staff engineers or PR team or guest writers?

A good example is Netflix Tech Blog (<https://netflixtechblog.com>).



Checklist /07

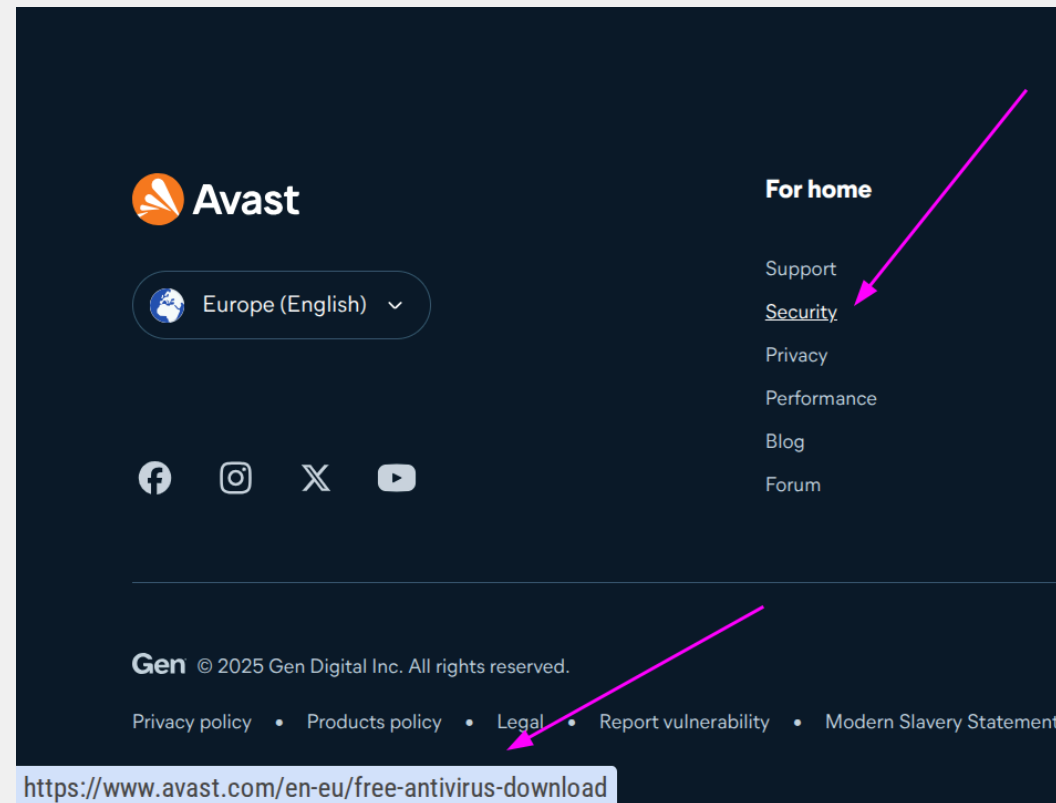
Do the company engineers regularly present at IT conferences? What kind of research do they perform?

Checklist /08

When was the company's privacy policy updated last time?

Checklist /09

Are public security materials written in marketing or technical language?



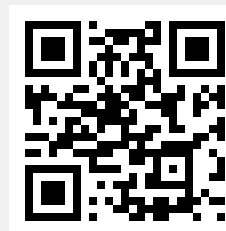
Checklist /10

Does the company have ever passed public security audits or shared audit reports?

Technical Considerations /01

Are security features a premium?

For example, how big is the "SSO tax"?



Technical Considerations /02

What technology stack does the company use?

Technical Considerations /03

"Red flags"

- Appliances
- Heavily-customized open-source

Technical Considerations /04

Does the company provide automated software updates for their product? How do they work?

Technical Considerations /05

How usable the documentation is?

An excellent example of writing technical documentation is ArchLinux Wiki (<https://wiki.archlinux.org>).



Other Considerations

- Does the product have a support channel or an active community of users?
- Does the product have any public source code that can be independently reviewed?
- Does the company have a security expert (at least according to LinkedIn)?
- Does the company have a record of past security incidents?
- What kind of incident response obligations does the company take?

The Developer's View

What constitutes security quality and makes others trust your product?

Security Quality

- ☑ Usable internal documentation and decision log
- ☑ Adherence to security standards (OWASP, etc)
- ☑ Use of infrastructure-as-code solutions
- ☑ Use of linting tools
- ☑ Use of SAST (static application security testing) tools

Showcase Your Efforts!

You do better than competitors (or at least not worse), but please tell your product owner and marketing team about that.

Final notes

Trust resides on knowledge and emotions.

We can not control what the others feel but we can transparently share information about our software to demonstrate its security maturity.

Thank You