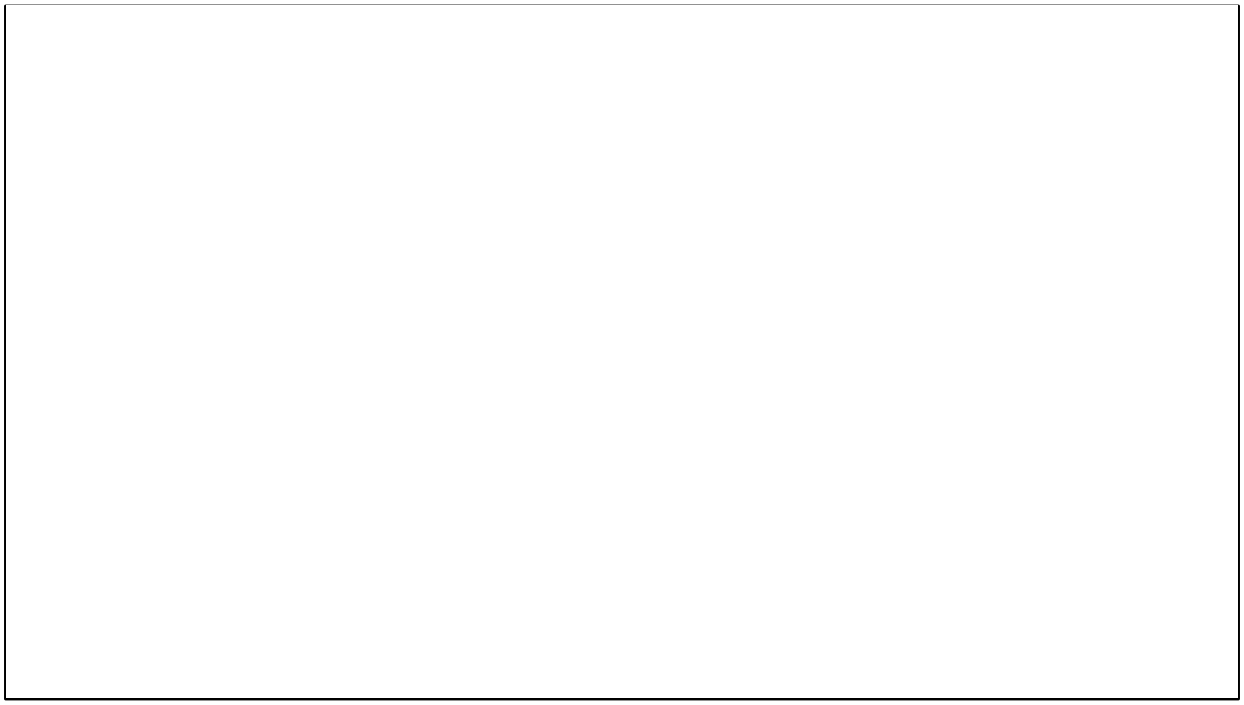
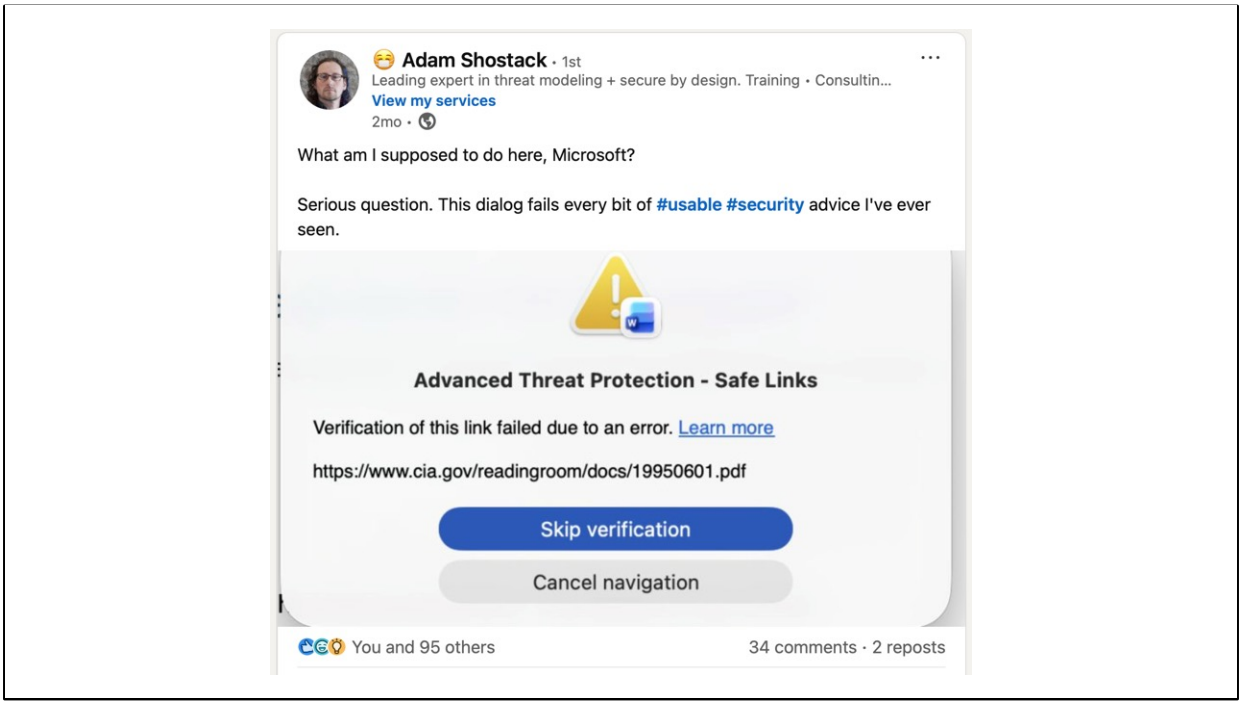
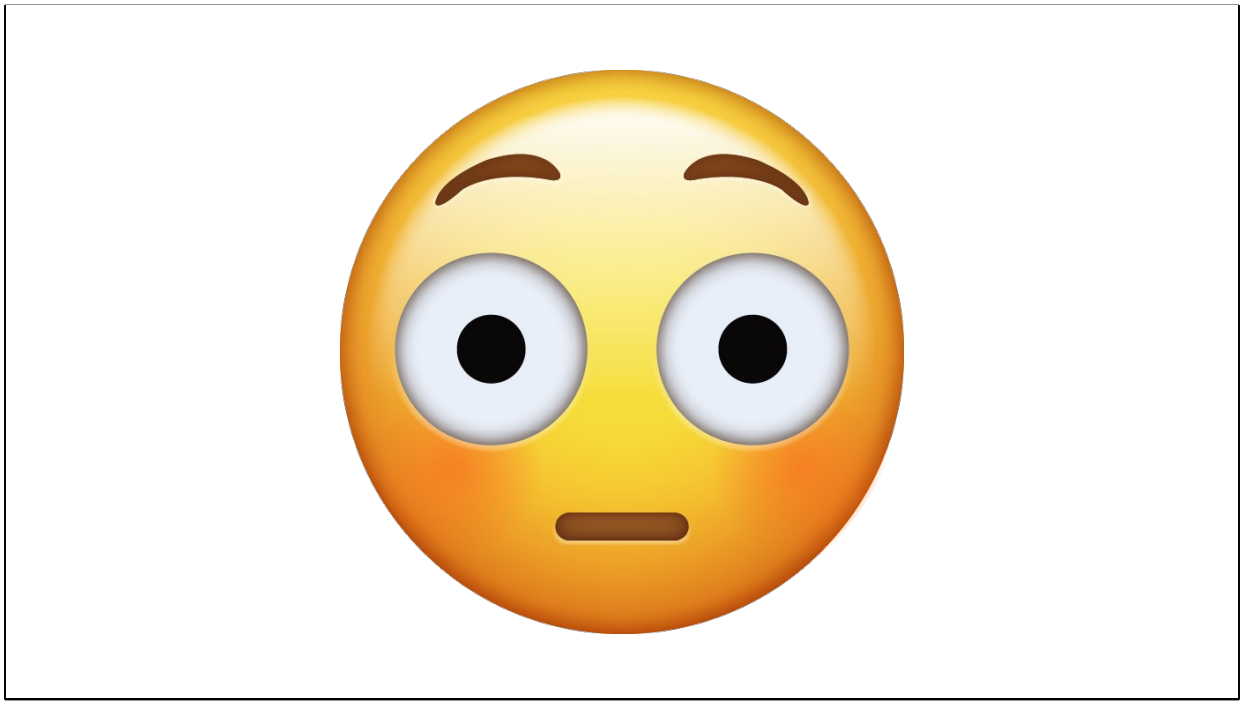


A few months ago, I saw a post on LinkedIn about a badly designed security warning.



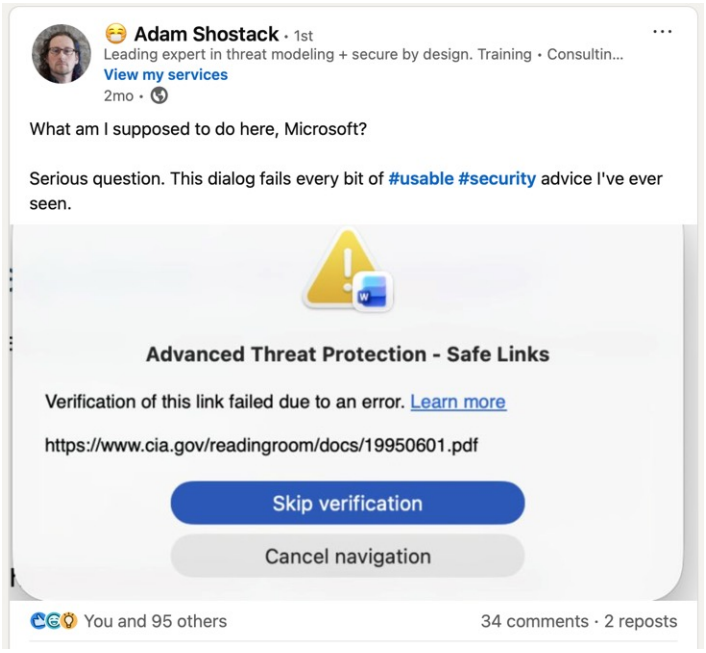
If you're like me, your reaction is something like...

Source/Image: https://www.linkedin.com/posts/shostack_usable-security-activity-7416636096668774400-qtOU/



Wat?

Image: https://emojiisland.com/products/flushed-iphone-emoji-jpg

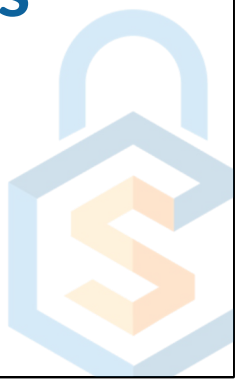


The irony here is that Adam Shostack was a coauthor of a Microsoft paper on how to write good security warnings that was published nearly 15 years ago (2012).

Source/Image: https://www.linkedin.com/posts/shostack_usable-security-activity-7416636096668774400-qtOU/

Cybersecurity Warnings

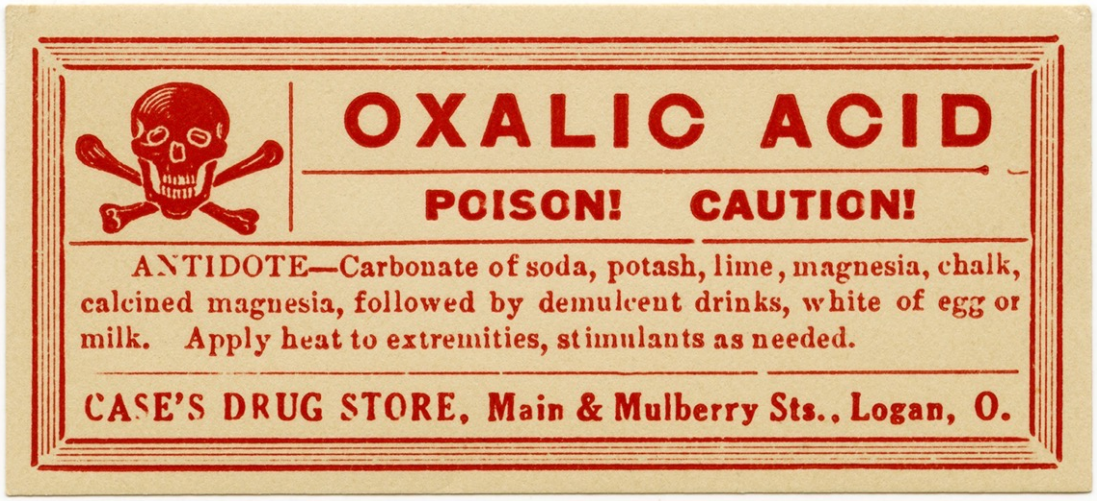
John Benninghoff
Security Differently



This talk came about because of an ongoing collaboration with a former coworker who led our UX team. Her PhD thesis was on safety warning labels.

I'll have a QR code at the end for you to download the slides with notes and links to all the references.

Let's start with a brief history of safety warnings and cybersecurity warnings.



Early safety warnings included poison warnings directed at consumers and warnings in factories to prevent worker deaths. "In 1927, the United States enacted its first federal warning legislation, the Federal Caustic Poison Act (FCPA)."

Source: Wogalter, M. S. (2006). *Handbook of warnings*. Lawrence Erlbaum Associates. https://www.routledge.com/Handbook-of-Warnings/Wogalter/p/book/9780805847246
Image: https://olddesignshop.com/2014/10/oxalic-acid-poison-label-free-vintage-clip-art/

Industrial warnings were first standardized in 1941, in ANSI Z35 (now Z535) - The radiation symbol was added in 1959 and biohazard in 1968.

Source: https://en.wikipedia.org/wiki/ANSI_Z35
Image: https://commons.wikimedia.org/wiki/File:Z35-1968_Sign_-_Danger_-_High_Voltage.svg
Bonus:
https://web.archive.org/web/20120213165520/http://www.hms.harvard.edu/orsp/coms/biosafetyresources/history-of-biohazard-symbol.htm

Importantly, safety warnings have been driven by employer and product liability that established a **duty to warn.**

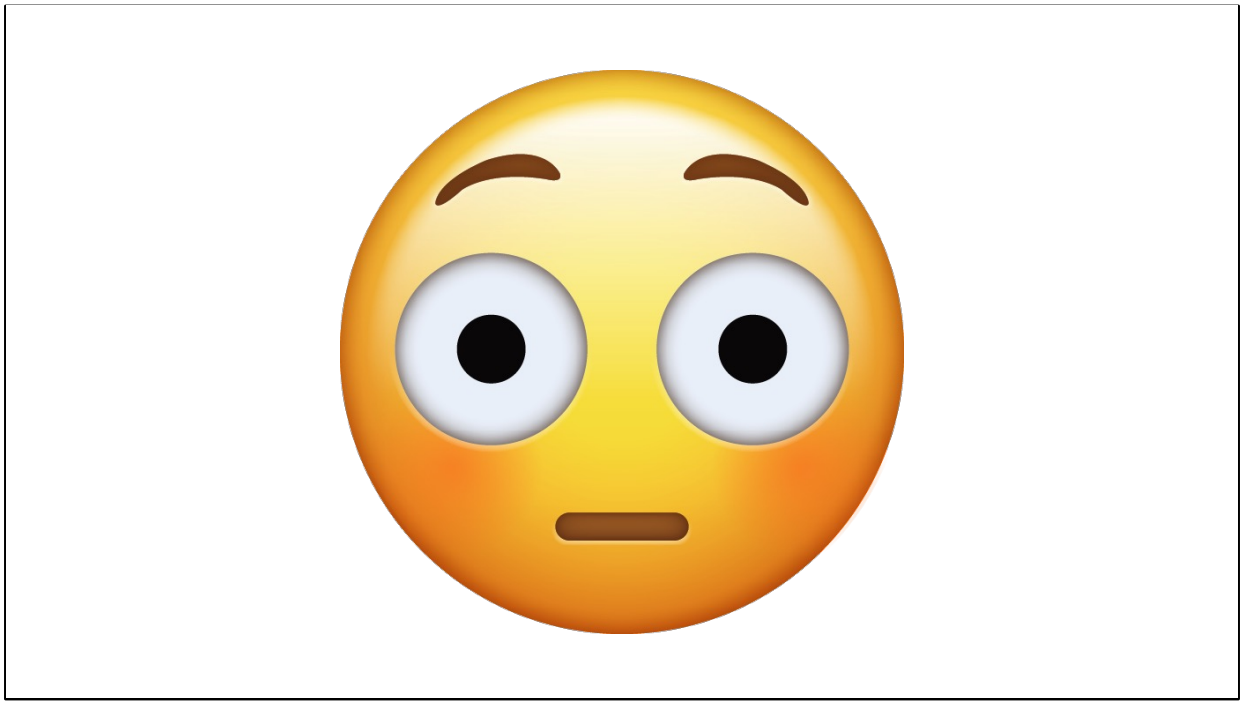
But, what about cybersecurity? Antivirus software, an early source of warnings, wasn't created until the 1980s. One problem: early antivirus software would sometime flag a benign file as a virus (false positive).

Source: Wogalter, M. S. (2006). *Handbook of warnings*. Lawrence Erlbaum Associates. https://www.routledge.com/Handbook-of-Warnings/Wogalter/p/book/9780805847246
Image: https://commons.wikimedia.org/wiki/File:16_CFR_§_1205.6_Warning_label_for_reel-type_and_rotary_power_mowers.svg

Figure 3-5. System Scan response options

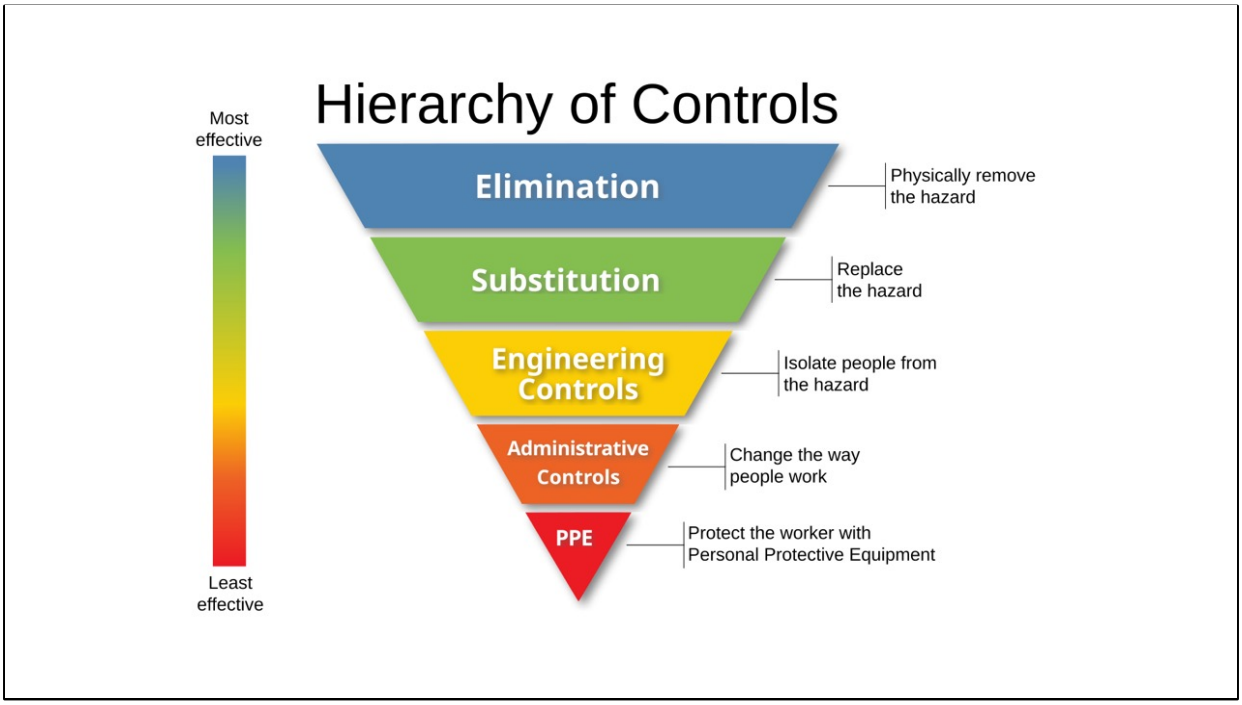
McAfee VirusScan, 1999. Clean = try to clean, Continue = ignore and keep scanning, Stop = stop scanning, Exclude = mark as safe and continue, Delete = only safe option. Again, if you're like me, your reaction is...

Image/Source: http://archive.org/details/mcafee-virusscan-for-windows-95-and-windows-98-users-guide-version-4.0.1



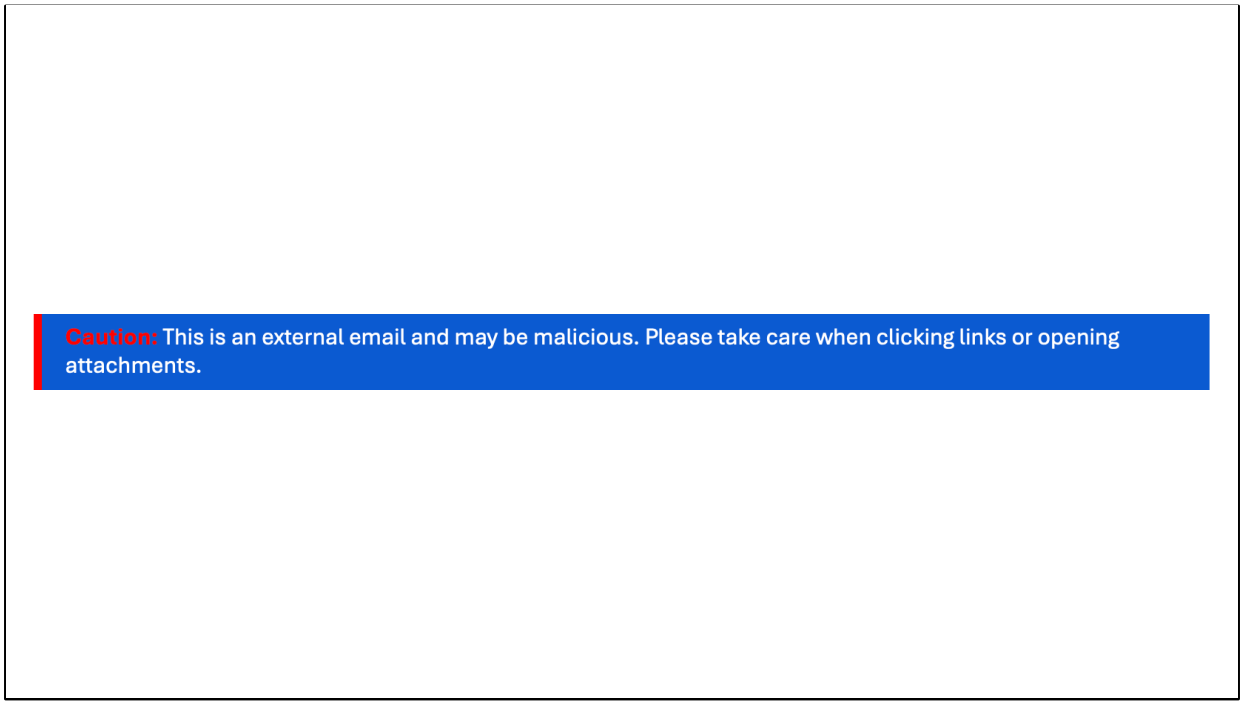
Wat?

Image: https://emojiisland.com/products/flushed-iphone-emoji-jpg



So, what can we learn from safety warnings? The Hierarchy of Hazard Controls is an idea from safety that's overdue to be adopted in technology. It's a reminder that warnings are the *least* effective control, and when a more effective control is feasible, it should be used instead (or in addition to). This can be simplified as: Design, Guarding, Warning.

Source: https://en.wikipedia.org/wiki/Hierarchy_of_hazard_controls, https://journals.sagepub.com/doi/10.1177/1557234X0600200109
Image: https://commons.wikimedia.org/wiki/File:NIOSH's_"Hierarchy_of_Controls_infographic"_as_SVG.svg

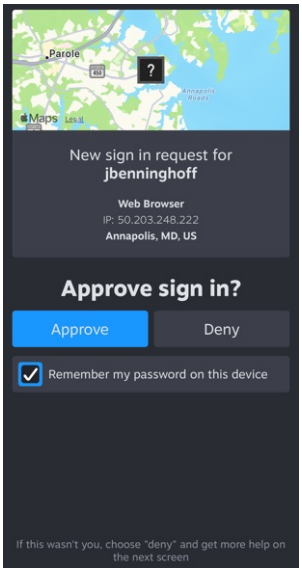


How many people get a warning like this in their email? How many still pay attention to it? How many change their behavior because of it? Story from school – discussion of a student forgetting to fold in the mirrors of their truck – most suggested some type of warning, except an Oil & Gas professional, who said “get a bigger garage”.

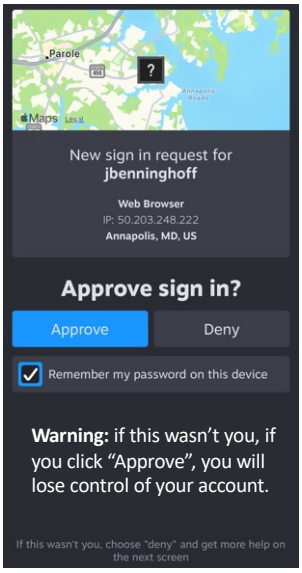
Phishing is better handled through guarding (blocking malicious emails) and design (phishing-resistant MFA = passkeys – Dan Lew’s talk at 11:35).

Explicitness: safety warnings are clear about the hazard and the potential consequences of an accident.

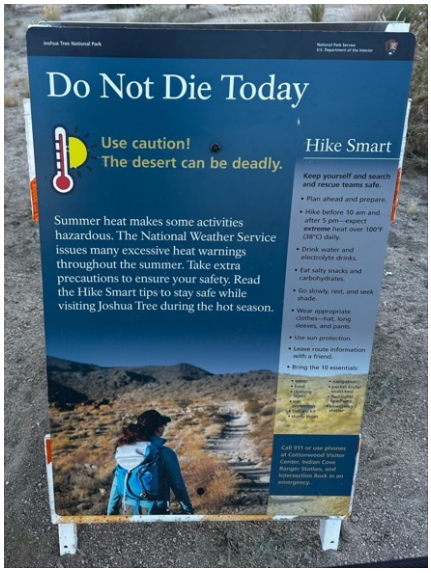
Source: https://journals.sagepub.com/doi/10.1177/1557234X0600200109
Image: https://commons.wikimedia.org/wiki/File:ANSI_Z535_Style_sign_Warning_010.svg



I took the picture on the left while hiking; again, the sign is quite explicit about the hazard and outcome. The screenshot on the right is a typical “approve sign-in screen.” (recognize it?)



We can add a better warning for the approve sign-on screen on the right!



Another example of an explicit warning that works.

Photo: Tony Martin-Vegue

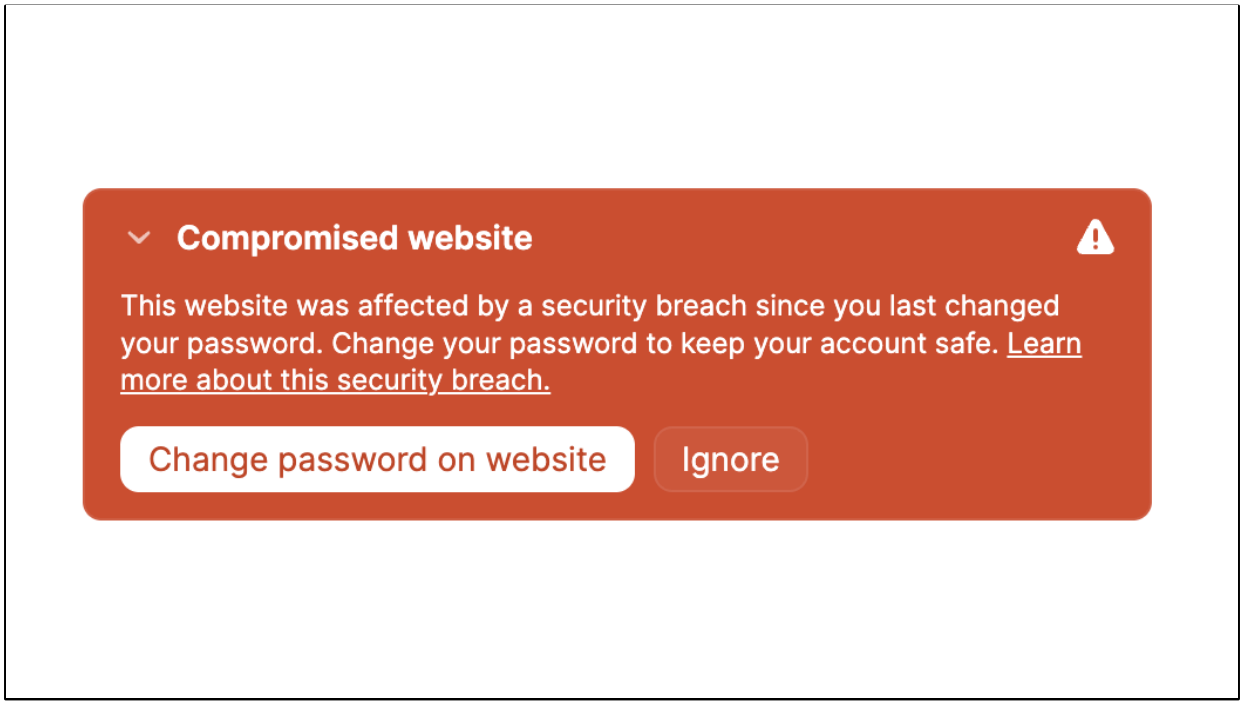
Cybersecurity Warnings

Examples: Action-Required, Judgement-Required

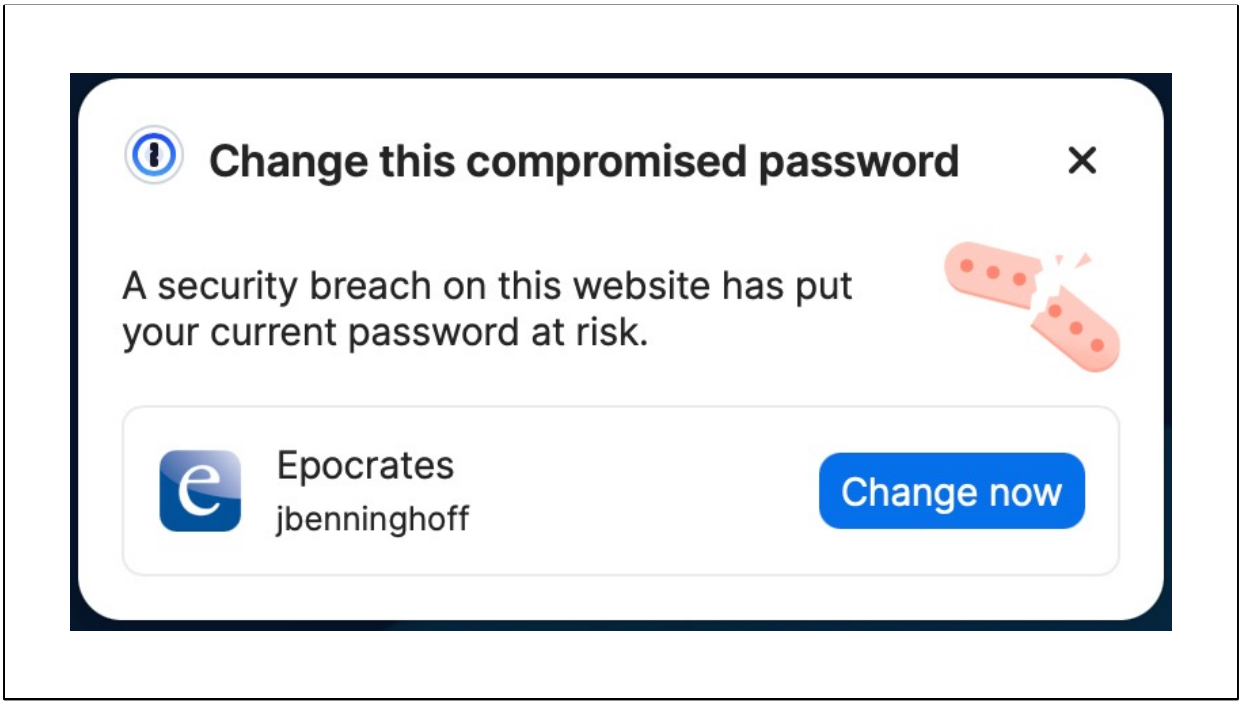
Key insight: there are two types of cybersecurity warnings:

Action Required: Hazard is known, but the user must act because the system can't.
Judgement Required: Hazard may or may not be present, and the user must make a risk decision.

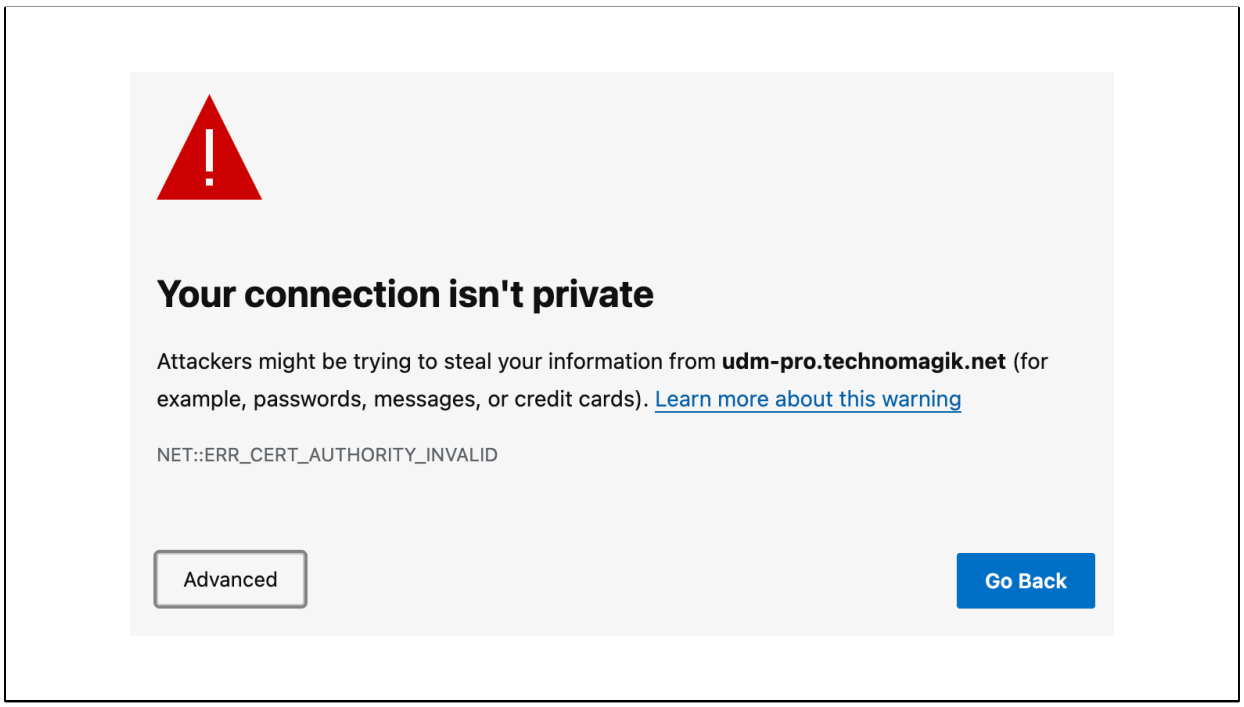
We'll look at examples of both, action-required first (less common).



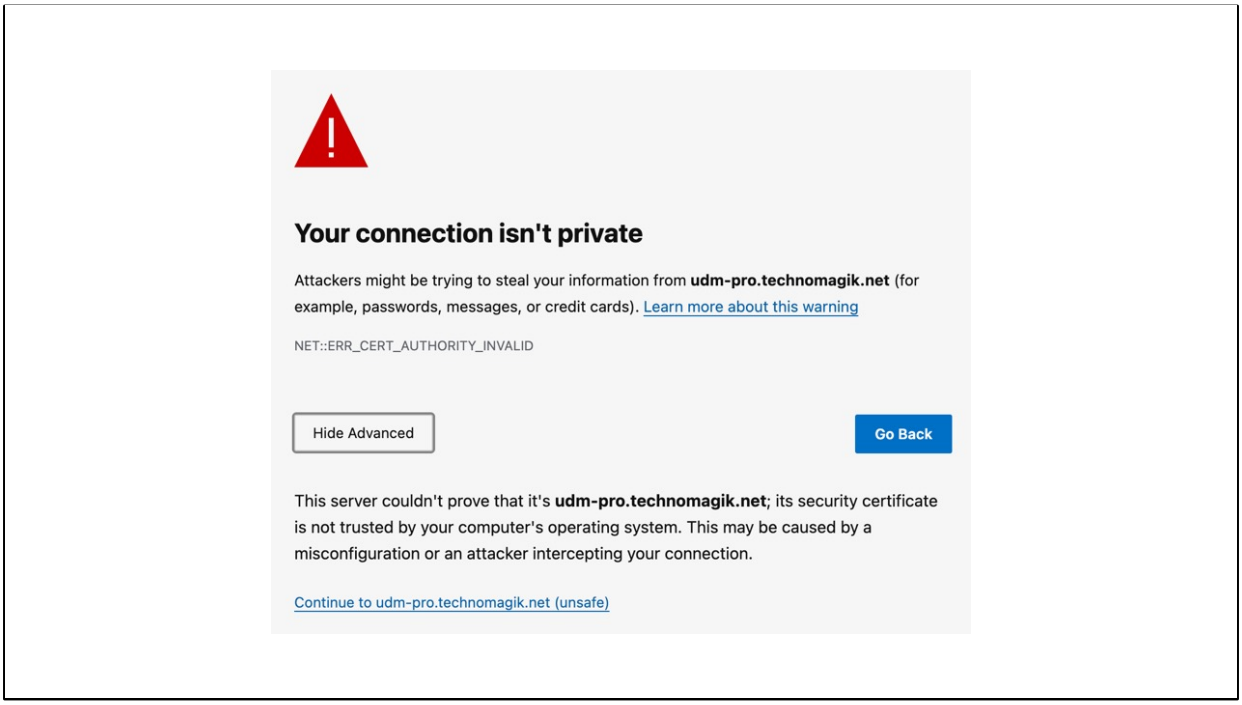
Action-required example: in the 1Password App, selecting a Login that has experienced a breach generates a warning banner above the Login entry. It's clear and explicit and makes it easy to act.



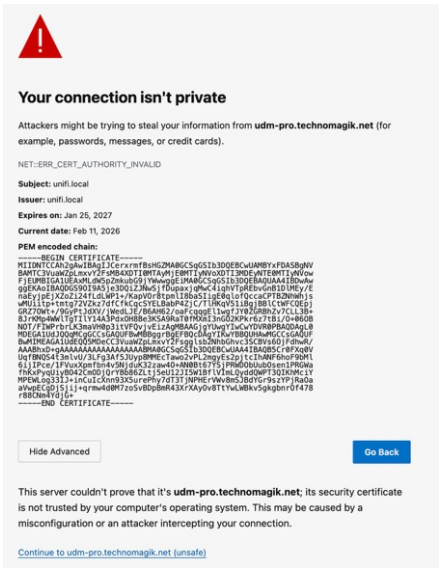
If the banner warning is ignored, 1Password displays an additional warning after autofilling the username and password, prompting a password change when it's most accessible. (Good design)



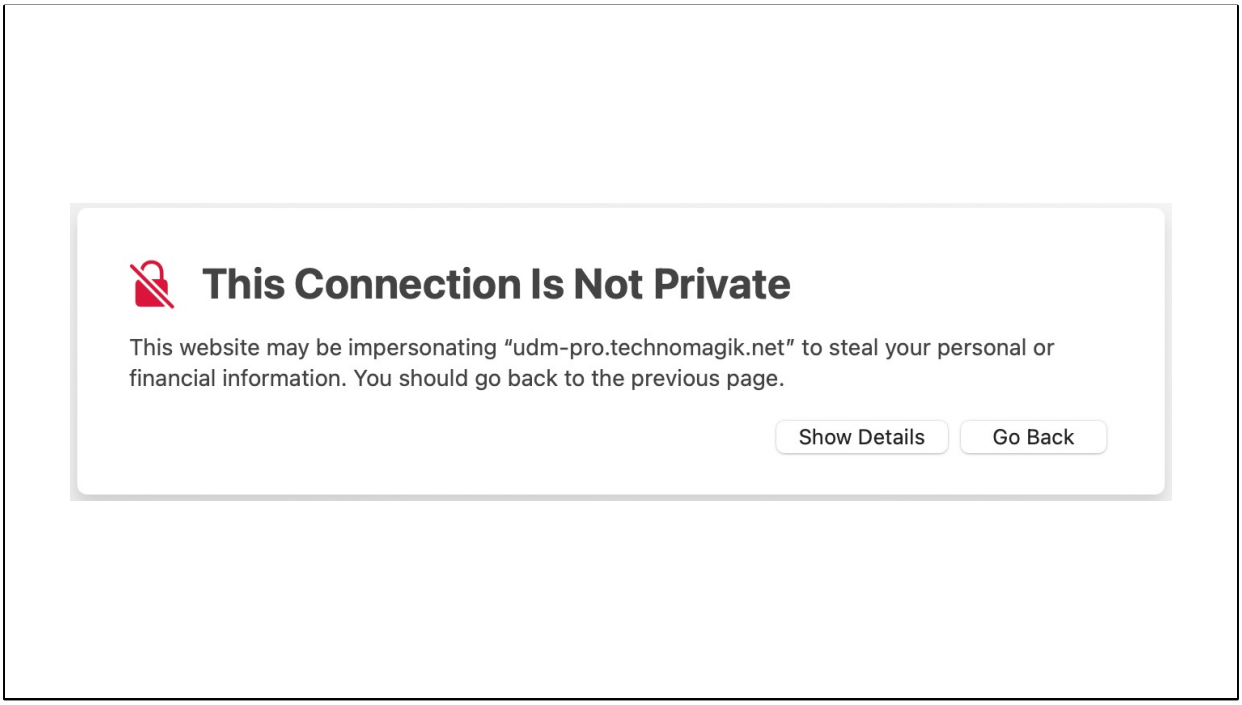
Judgement required example: Microsoft Edge certificate warning. It uses some gating (must click Advanced to continue).



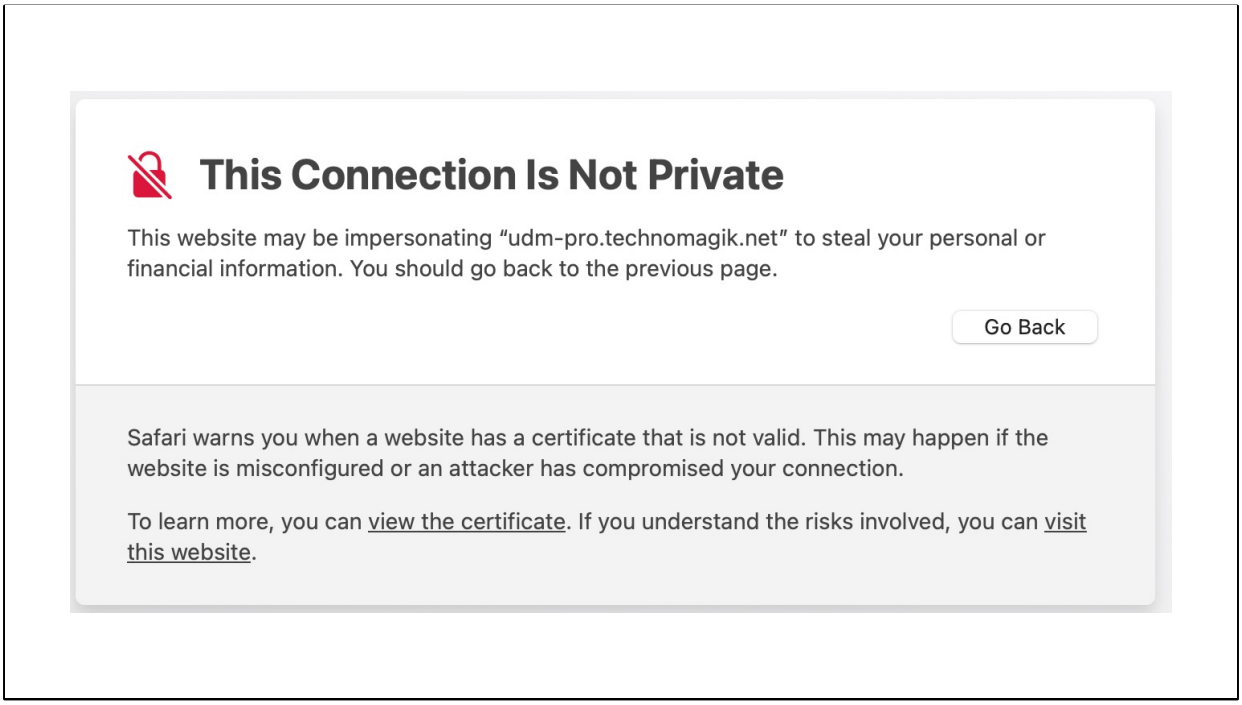
This is somewhat explicit but uses jargon and doesn't describe the most common scenarios (self-signed or expired cert vs small chance of listening in). Also, where's the certificate? I might need that information to decide..



Clicking on “NET:ERR_CERT_AUTHORITY_INVALID” reveals some certificate information. Why is this hidden?

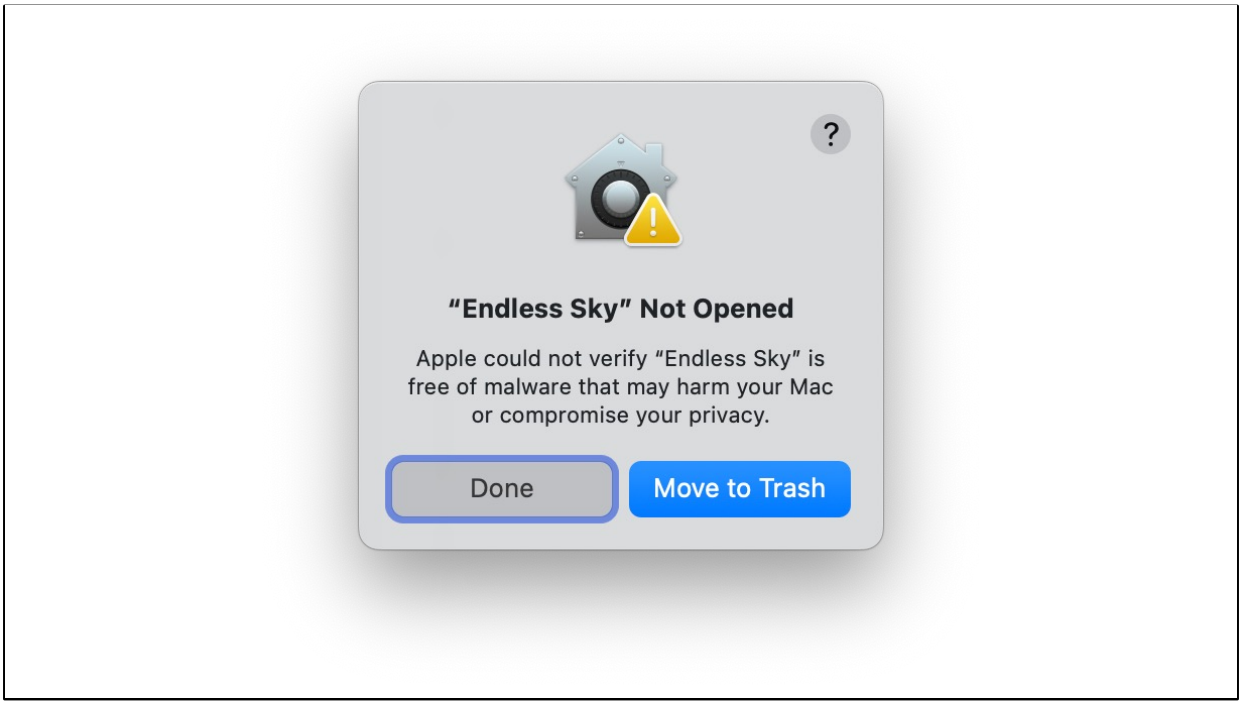


Safari certificate warning. How does this compare?



A bit more explicit, but the language could be cleaner and include common examples (self-signed certificate).

Safari shows you the entire certificate, which is better; you can see that the cert is self-signed.

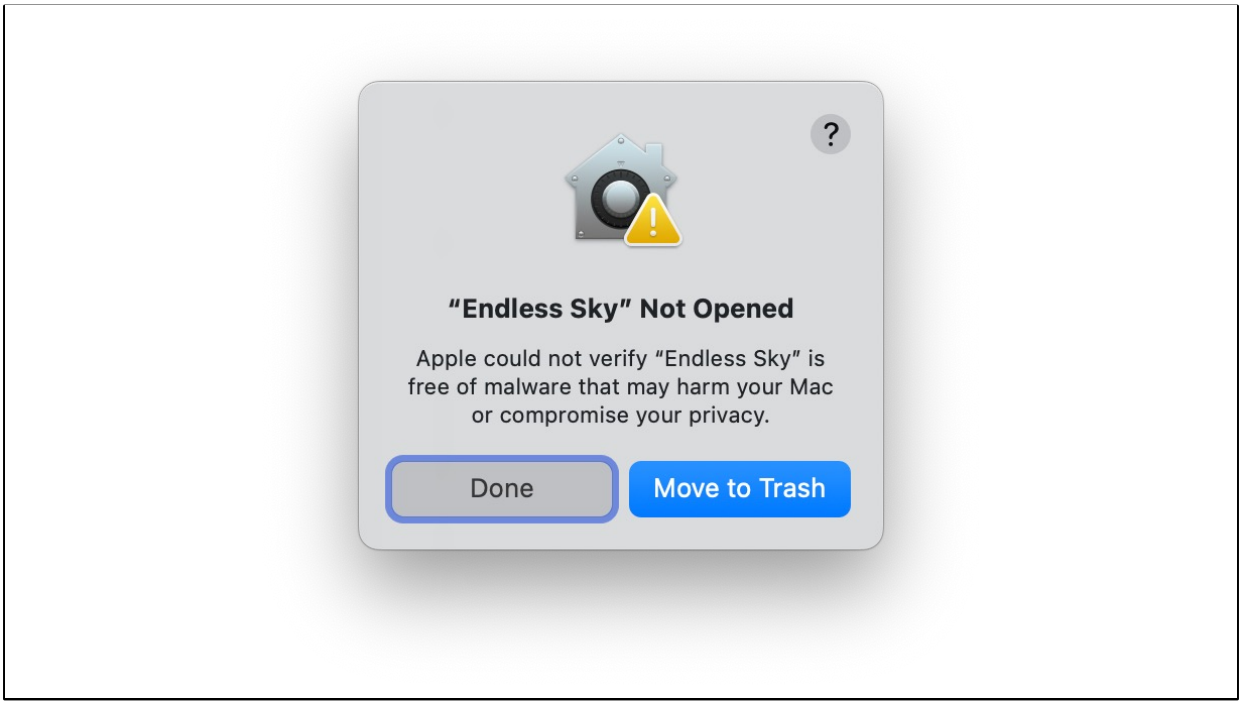


This is one of the most sophisticated security warnings I've found! This warning appears when opening an unsigned application on macOS.

I bet you're thinking something like this...

I bet you’re thinking something like this…

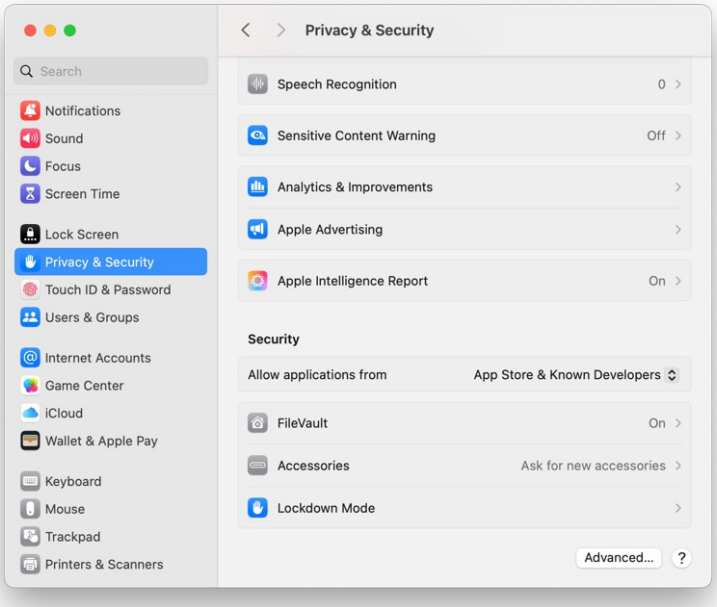
Image: https://emojiisland.com/products/unamused-iphone-emoji-jpg



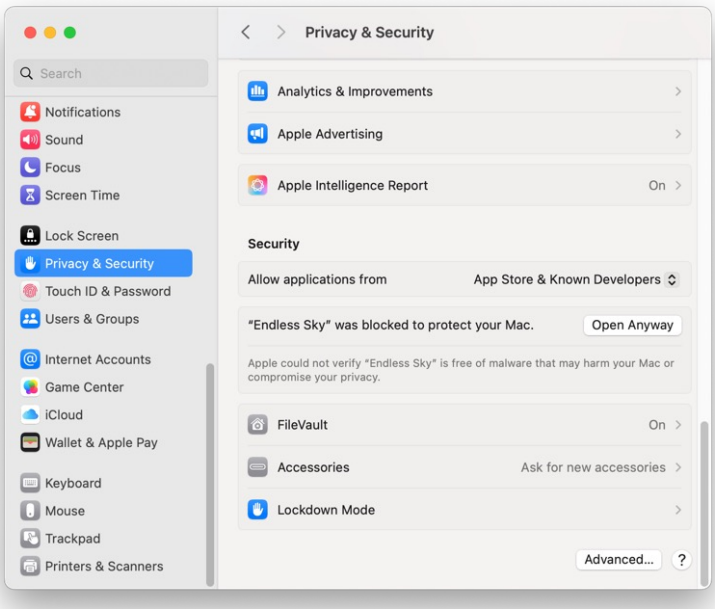
What makes this warning sophisticated? It's Necessary, Explicit, and only offers safe choices. But what if you understand the risks and want to run an unsigned application anyway?

IYKYK!

There's hidden gating here – if you know how macOS security works, you can bypass the warning. This is a way of gating based on the user's knowledge, to see if they are "qualified" to make an informed decision to ignore the warning.



This is what the Privacy & Security tab in System Settings normally looks like.

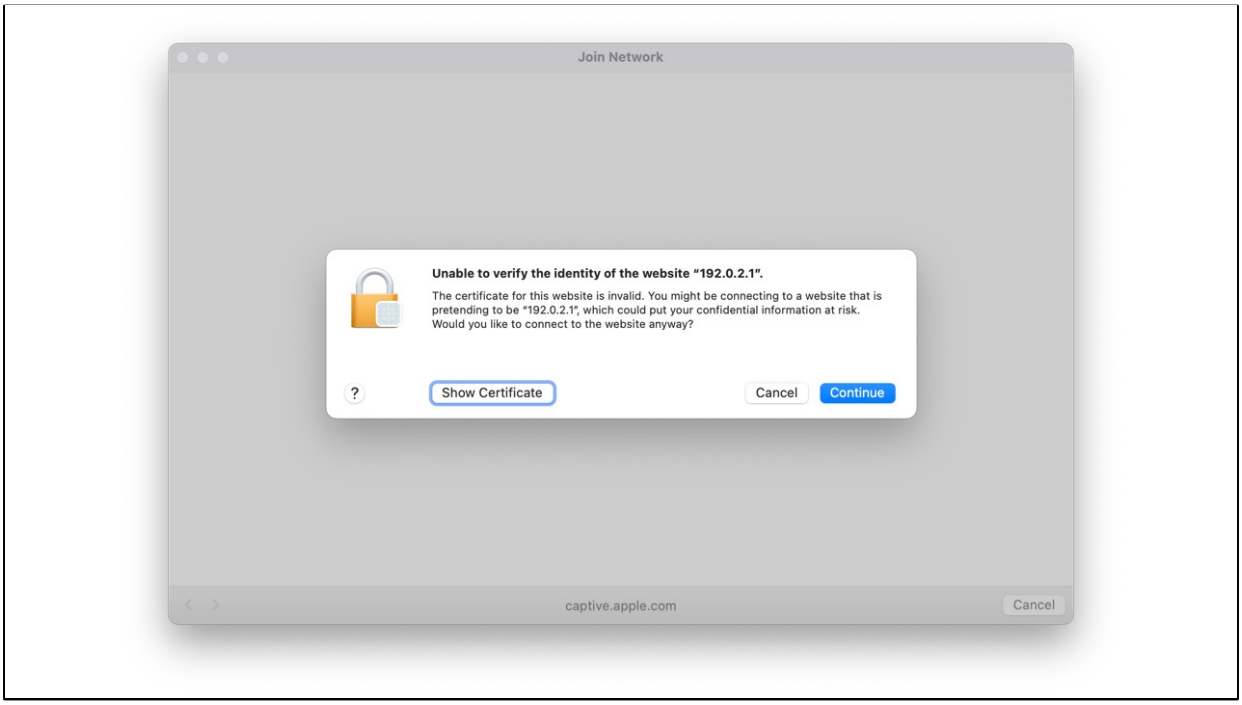


After you try to open an unsigned application, an extra setting will appear here – if you know it's there, you can bypass the gating and open the application.

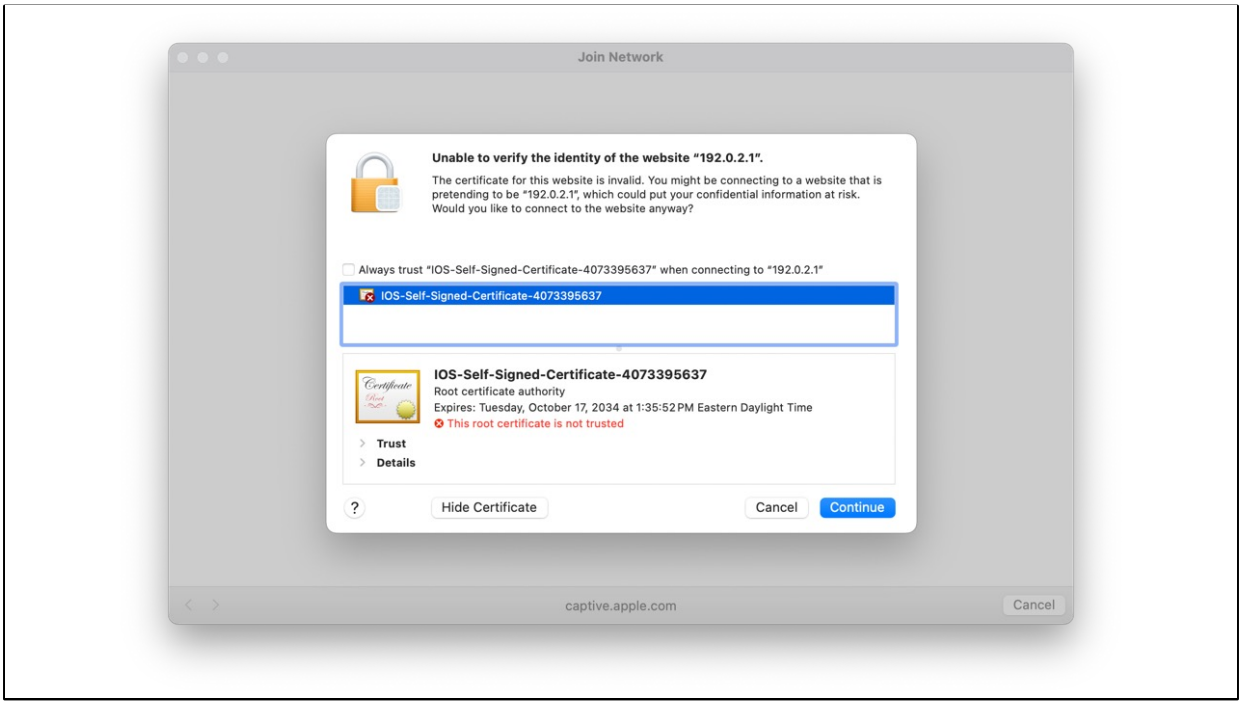
Lightning Round!

Let's ~~mock~~ see some more examples!

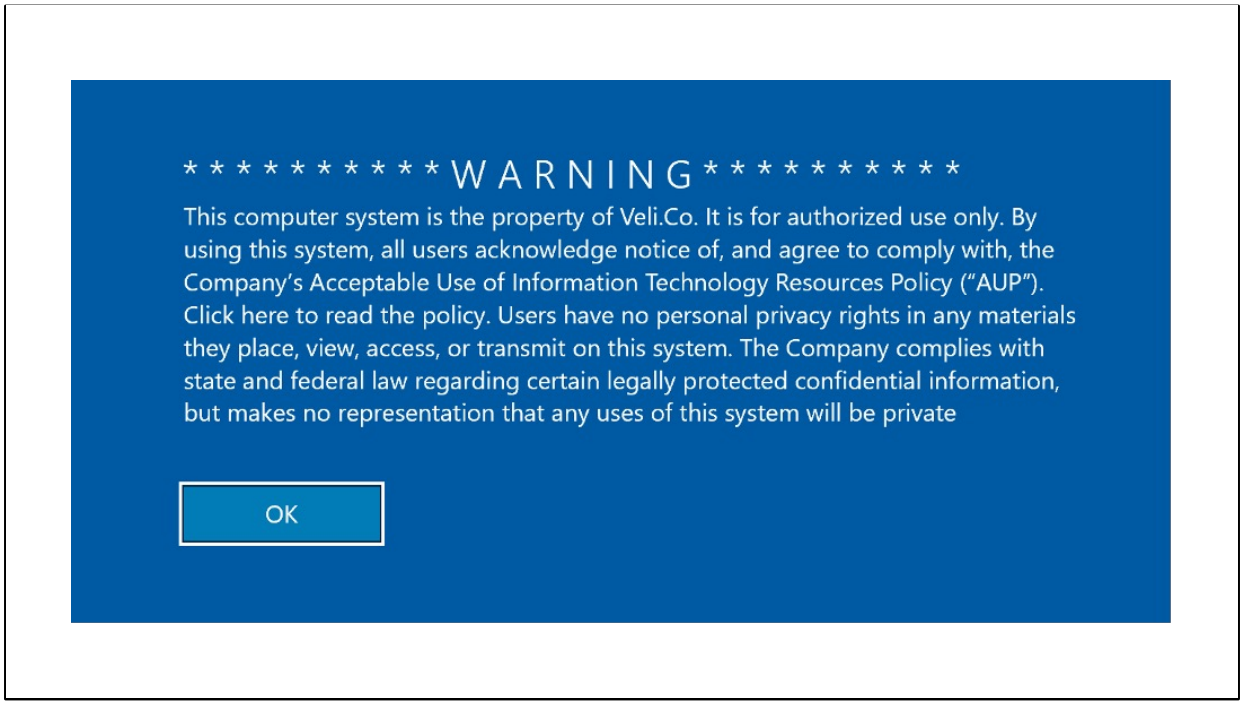
And...



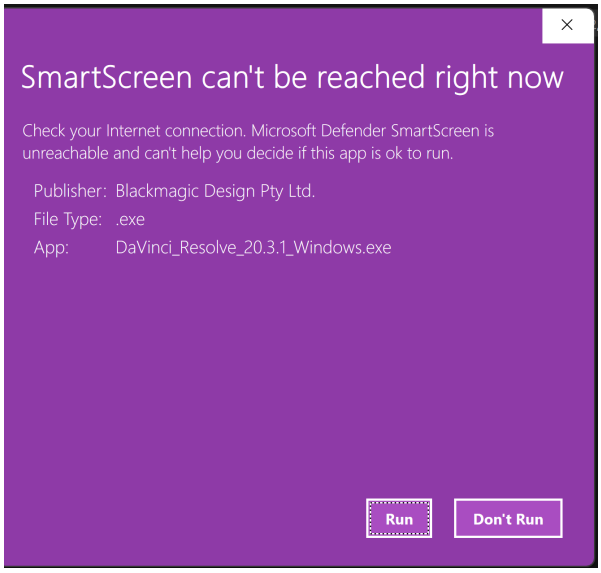
This is a warning I got when connecting to Wi-Fi at a conference…



In this case, IOS = Cisco IOS. Why?



Warning banners…they're terrible and are based on a security urban legend that if you don't have them, you can't prosecute…

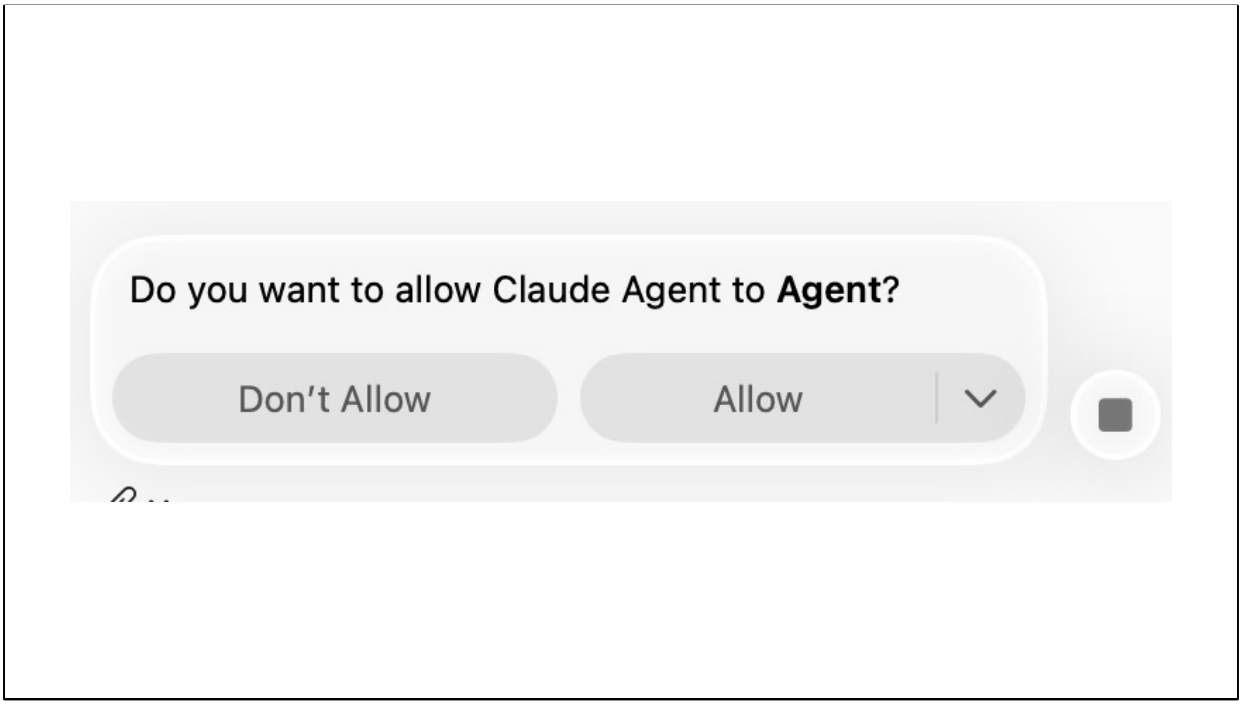


Why are we even seeing this message? This could be solved through improved design.

This isn't even a security warning, but a couple people asked about it, so I'm including it!

Source: https://en.wikipedia.org/wiki/Guru_Meditation
Image: https://commons.wikimedia.org/wiki/File:Amiga_Guru_Meditation.gif

And our winner...



Screenshot: Graham Wood

Thank you!

Exposed Technology	Increased Claims Likelihood
Cisco ASA device	**x4.7 – 11.6** [3,5]
Citrix VPN	**x11.6** [5]
Fortinet device	**x3 – 5** [1,5]
VPN panels	**x3 – 4** [4]
Pulse Secure VPN	**x2.6** [2]

*IP count is also in with a shout
Sources: [1] Coalition, 2023; [2] Bitsight, 2023; [3] Coalition, 2024; [4] Coalition, 2026; and [5] AtBay, 2024

This has nothing to do with warnings, but if your organization uses VPNs, they should know that companies with VPNs and other perimeter security devices are much more likely to file a cyberinsurance claim. You are safer using the internet (and appropriate controls, like MFA) than an "internal" network! (Thanks to Daniel Woods!)

Source:
https://www.linkedin.com/feed/update/urn:li:activity:7454125124451995648/

Slides, Connect & Website

Slides:
jbenninghoff.com/qr

Connect:
linkedin.com/in/jbenninghoff/

Website:
jbenninghoff.com
security-differently.com

Scan the QR code for slides and more!