Beware of website hackers: Developing an awareness video to warn for website hacking

Anne Hennig
Karlsruhe Institute of Technology (KIT)

Leoni Schmidt-Enke
Karlsruhe Institute of Technology (KIT)

Miriam Mutter
Karlsruhe Insitute of Technology (KIT)

Peter Mayer
University of South Denmark (SDU)
Karlsruhe Insitute of Technology (KIT)

Abstract

Websites that are not well maintained can be vulnerable to hackings. One type of hacking that might occur is embedding redirects to fake shops into legitimate websites. We created an awareness video to address these hacking. We first conducted a content analysis to collect relevant information. We then created a video based on this information and evaluated the video with four focus group interviews with overall 13 participants from different areas of expertise. The constructive feedback from the experts allowed us to improve the video.

1 Introduction

Hacker gaining unauthorized access to websites is a huge problem [6]. Such unauthorized access can incur various kinds of hackings, like comment spamming, defacement of websites or redirects [3]. While most attacks are immediately noticeable (e.g. defacement, or spread of malware), some rather unknown attacks are not easy to recognize. We identified domains that are used by hackers to redirect to malicious websites, e.g. fake online pharmacies, fake online casinos, or porn websites. Sucuri[1] describes this kind of hacking as search engine Spam or SEO Spam [7]. To place the redirect on a website, a hacker need write access to the website.

In previous work [5] we found that notifying website owners about this type of hacking is difficult. The redirect is only apparent when opening the link from a search engine, and most website owners are not aware of the hacking. Thus, raising awareness for the severity and possible consequences of the hacking is important. We decided to design an awareness video because previous research found videos to be by far the most preferred delivery method for ISA (e.g. [1, 2]).

The aim of our research was to identify relevant information on this type of hacking from existing sources of information in a first step and then develop two awareness videos on the basis of these information. The video we present in this work, focuses on the identification and explanation of the hacking, whereas video B will focus on measures and prevention[2]. We then evaluated the video through expert feedback.

2 Content Analysis, Video Development, and Evaluation

Methodology Content Analysis As first step, we conducted a content analysis of videos on YouTube and of news articles as well as scientific papers, which we identified based on a structured literature review. Six keywords were extracted from a blog post [7] that we found was related to the hacking we wanted to describe: SEO Spam, Pharma Hack, Redirect Hack, Wordpress Hack, Spam Injection, Spamdexing.

We used these keywords to search for English and German videos/articles in the YouTube video search, the academic databases Science Direct, IEEEExplore, SpringerLink, ACM, and Emerald, as well as the Wiso database for news articles. We found 84 videos, 184 papers and 39 news articles which were then again filtered for duplicates, relevance and language[3]. In the end, 45 videos, 39 news articles and 1 paper were completely analyzed[4]. We used inductive coding for the analysis of the materials, and the codebook was developed with four coders and two independent testers.

[1] https://sucuri.net/

[2] Video B is not produced yet, and will, therefore, not be part of the following evaluation.

[3] E.g. papers that described new methods to improve search engine algorithms or videos that had an English title but were recorded in another language were excluded

[4] All other papers were excluded due to duplicates or because they only used the keyword(s) as example of how search engine algorithms are tricked without giving definitions or explanations.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

Results Content Analysis The type of hacking we are investigating is sparsely described in the academic literature. Only one paper [8] was relevant for the analysis, but other than a description possible hacking attacks on websites, no advice was given how to identify and remediate this specific type of hacking or how to protect from future hackings. We could also not deduce any relevant content from the news articles. The majority of the Youtube videos were screencasts[5] (40.0%), followed by tutorials[6] (20.0%), and recorded talks or webinars[7] (13.3%). Only two videos were coded as explanatory videos, but no animations were used in either.

The type of hacking is described with a number of different terms. Furthermore, some videos use different terms synonymously (e.g. "SEO Spam" and "Spamdexing"), or the same term is used to explain different hackings across videos (e.g. "redirect hack"). Repercussions for website owners are rarely mentioned (26.7%), and even fewer videos mention repercussions for users (8.9%). Two third of the videos do not explain the motivation of hackers, and only about half of the videos (55.6%) describe indicators of compromise. Nearly a third of the videos were identified as commercial videos (31.1%), advertising a product (esp. malware scanner) or website services. More than 60% of the videos were identified as non-commercial, but – again – for more than 40% of these produced videos self-promotion was identified.

Awareness Video We used the results of the content analysis to develop a three-minute explanatory video using 2D animation. We decided to only refer to the attack as "hacking", since we found that to describe the hacking inconsistent terms and definitions are used. We also decided against introducing a new term or definition for the hacking to not confuse users further. See Appendix A for the final story board.

Methodology Focus Group Interviews To evaluate the video, we recruited 13 domain experts for focus group interviews. The participants had different backgrounds[8] and we conducted four online focus group interviews between January 30 and March 3, 2023. The focus groups followed a semi-structured interview guideline to answer the following questions: (A) Are the information given in the video correct and complete? (B) Is the design and the presentation of the information appropriate? (C) Is there any general feedback? As described by Dell et al. [4], participants might be biased towards an artifact the interviewer created. To meet this bias, we explicitly asked for missing and/or incorrect information and gave the participants plenty of time to also express concerns or reservations. We used verbatim transcription and analyzed the interviews with a codebook that was developed by three coders.

Results Focus Group Interviews In general, participants liked the style and the way we presented the information. They did not find any critical errors and mainly agreed that the most important information was presented.

We also received suggestions for improvements. In three of four groups, it was discussed that the identification of the hacking via the site search operator "site:" is not prominent enough or will not be understood by the users. It was suggested to emphasize that the operator is needed to identify the hacking[9]. In one group the length of the video was criticized and it was suggested to create a shorter version of the video for a quick overview to meet the needs of different target groups. Also, in three of the four groups it was criticized that information on the remediation of the hacking as well as preventive measures are missing. It was considered important that this information is provided. The groups further agreed that the second video is needed to provide a comprehensive description of the hacking.

3 Future Work

We found two recommendations most crucial: Firstly, we need to make sure that the identification of the hack via the site search operator "site:" is made more prominent. It is currently not decided whether these changes will already be made in the first video or further addressed in the second video. Secondly, concerns were raised that the video cannot stand on its own. Thus, the video will not be made public before the second video is also produced. We also share the concern that adjustments are needed to meet the needs of different target groups. Future work will investigate how these adjustments can be implemented and to what extent it is necessary for different target groups. We also got suggestions on what to include in the second video: All groups discussed if information on other forms of website hacks should be mentioned. For this, it might be necessary to conduct an extended content analysis with different keywords to better understand which kind of website hacks are relevant to include in the second video.

Acknowledgments

This research is supported by the German Federal Ministry of Education and Research as part of the INSPECTION project (Zuwendungsnummer 16KIS1113), and by funding from the

[5] One person demonstrating a problem by recording their screen.

[6] Unlike screencasts, a speaker is present in a tutorial, and screenrecordings are - if at all - only used for demonstration purposes.

[7] Talks or webinars are usually longer with a speaker holding a lecture-like talk. Interaction with the audience in the form of, e.g., Q&A is possible.

[8] industry, German Federal Office for Information Security (BSI), Chamber of Commerce and Industry (IHK), Chamber of Crafts, State Office of Criminal Investigations (LKA), stakeholder groups for industry and small businesses in Germany

[9] Currently, searching with the "site:" operator is only shown in the pictures and the voiceover explains that one should search explicitly for their own website, not mentioning the operator.

topic Engineering Secure Systems, topic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs. Special thanks to Lauritz Kanyi, who was the second coder for the content analysis and contributed to the research as part of his job as a student assistant.

References

[1] Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, 2012.

[2] Yusuf Albayram, John Liu, and Stivi Cangonj. Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager. *European Symposium on Usable Security 2021*, pages 89–104, 2021.

[3] Cosmin A. Conţu, Eduard C. Popovici, Octavian Fratu, and Mădălina G. Berceanu. Security issues in most popular content management systems. In *2016 International Conference on Communications (COMM)*, pages 277–280, 2016.

[4] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. "Yours is Better!": Participant Response Bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, page 1321–1330, New York, NY, USA, 2012. Association for Computing Machinery.

[5] Anne Hennig, Fabian Neusser, Aleksandra Alicja Pawelek, Dominik Herrmann, and Peter Mayer. Standing out among the daily spam: How to catch website owners' attention by means of vulnerability notifications. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–8, 2022.

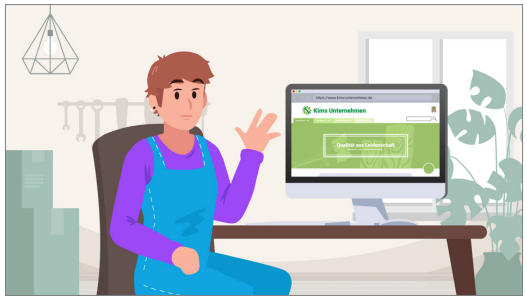
[6] Ranjita Pai Kasturi, Jonathan Fuller, Yiting Sun, Omar Chabklo, Andres Rodriguez, Jeman Park, and Brendan Saltaformaggio. Mistrust Plugins You Must: A Large-Scale Study Of Malicious Plugins In WordPress Marketplaces. In *Proceedings of the 31st USENIX Security Symposium*, pages 161–178, Boston, MA, 2022. USENIX Association.

[7] Art Martori. Spamdexing: What is SEO Spam and How to Remove It, 2 2020.

[8] Patchmuthu Ravi Kumar, Perianayagam Herbert Raj, and Perianayagam Jelciana. A Framework to Detect Compromised Websites Using Link Structure Anomalies. In Saiful Omar, Wida Susanty Haji Suhaili, and Somnuk Phon-Amnuaisuk, editors, *Computational Intelligence in Information Systems*, pages 72–84, Cham, 2019. Springer International Publishing.

A Story Board Video

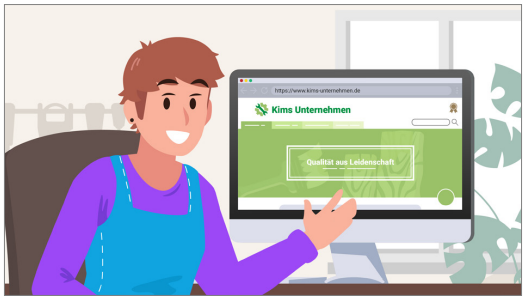
1



VOICE OVER
This is Kim

ANIMATION
Kim sits in front of their desk and waves.

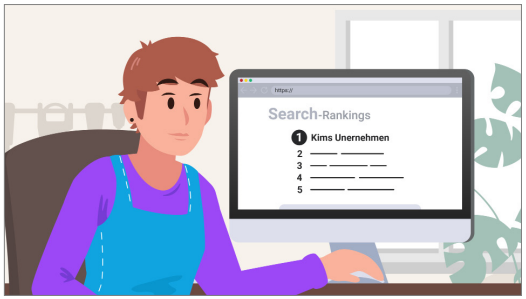
2



Some time ago, Kim set up a website for their own company -

ANIMATION
Zoom in: Kim happily shows the website of Kim's company. (kims-unternehmen.de)

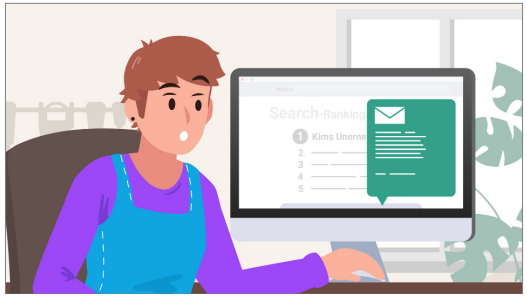
3



and has already been able to secure some good search engine rankings.

ANIMATION
The screen shows how Kim's company is increasing in the search engine rankings.

4



But one day, Kim is alerted via e-mail about something strange:

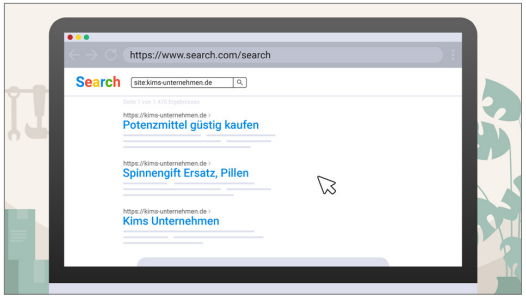
ANIMATION
An e-mail pops up in the corner of Kim's screen.

5

If you search the Internet explicitly for Kim's company website -

ANIMATION
Zoom into the monitor: "site:kims-unternehmen.de" is typed into the search engine.

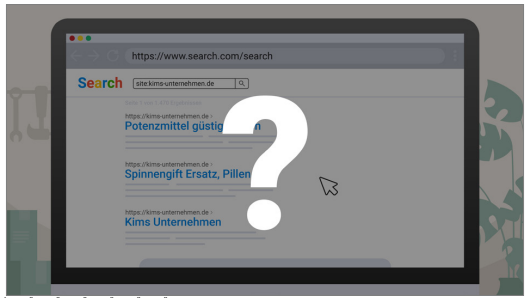
6



unusual entries appear, redirecting to a dubious online store.

ANIMATION
Results appear. But all of them show dubious pharmaceutical websites. Above each the URL in small letters: kims-unternehmen.de
Only the lowest entry is actually from Kim's website.

7



What has happened to Kim's website?

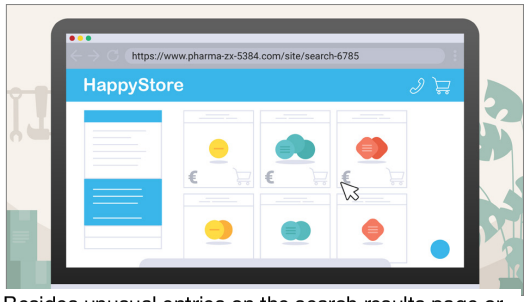
ANIMATION
Question mark appears.

8

Around the globe, more than 90,000 websites get hacked every day.

ANIMATION
Pop-up with globe appears. Little monitors with skulls all around. Pop-up disappears again.

9



Besides unusual entries on the search results page or redirects to dubious online shops, typical indicators are -

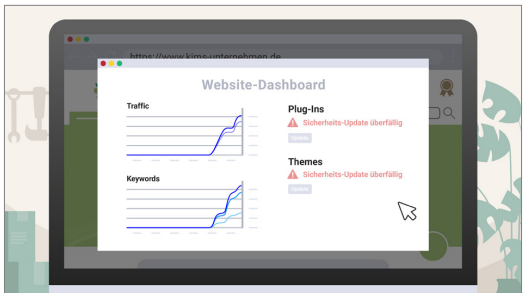
ANIMATION
Mouse click on the top search result (Figure 6). Online store for sexual enhancers appears.

10

an inexplicably high or sudden increase in website visitor numbers.

ANIMATION
Kim's website appears. In front of it a window with the traffic statistics.

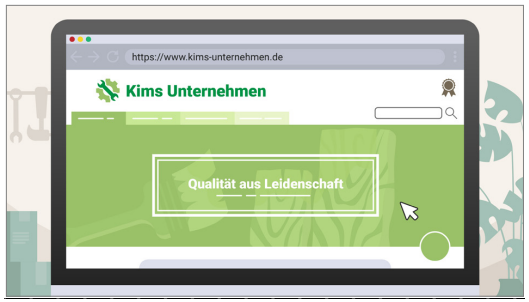
11



Typical gateways are, for example, vulnerabilities in the websites or weak administrator passwords.

ANIMATION
Traffic window scales to full screen. Right to the graphs, plugins and themes are marked with "Security updates overdue!"

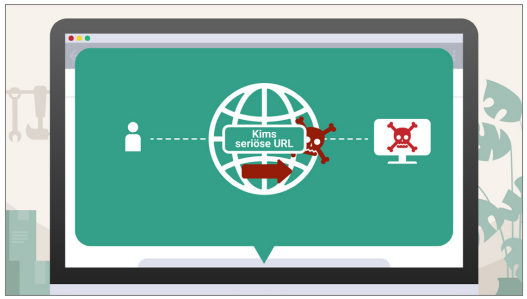
12



This way, hackers get access to the web space or even the whole web server.

ANIMATION
We see Kim's website.

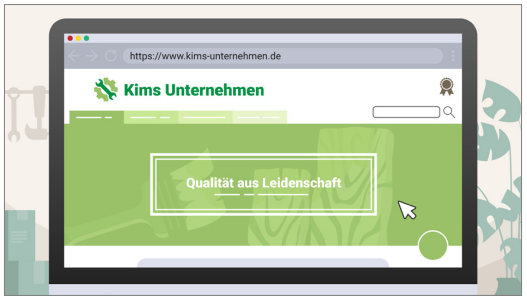
13



In the form of hacking that affected Kim, the attackers use the hijacked web space to place redirects to other websites.

ANIMATION
Fade in: Kim's web space (wire frame globe) appears. It reads: "Serious URL from Kim". A skull hides behind it. Arrows appear above it. Point/visitor flies from the left into Kim's website, but is guided by the arrow to the unsecure webspace (screen with skull), which suddenly appears.

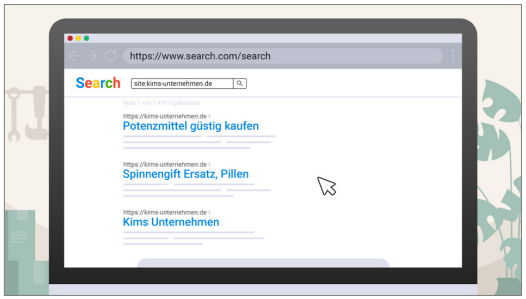
14



The changes are not visible on Kim's business website and, therefore, remain undiscovered.

ANIMATION
Back to Kim's website. Everything looks normal.

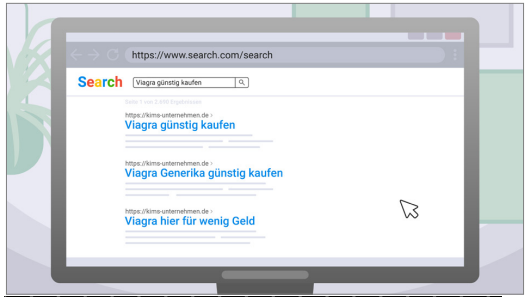
15



Only by looking at the search results page it is revealed that something is wrong with Kim's website

ANIMATION
Back to the search engine: search results for "site:kims-unternehmen.de" (as in Figure 6).

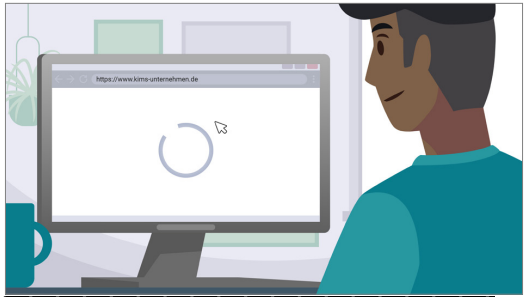
16



The hackers take advantage of the search engine rankings of the hacked websites in order to use the good ranking of legitimate websites for their illegal pages.

ANIMATION
Switch to another monitor in the visitor's room. Now "buy Viagra cheap" is entered in the search field. Kim's URL appears in the new results

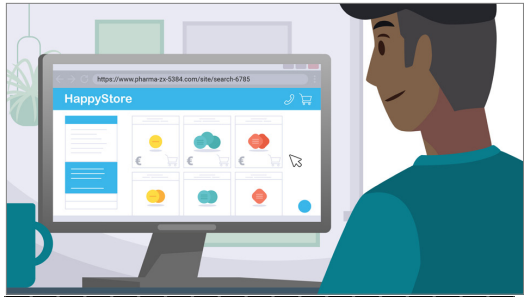
17



Visitors who follow one of the search engine links in good faith,

ANIMATION
Zoom Out. Visitor clicks on the top link. Kim's URL appears briefly in the bar and it loads. Very short moment.

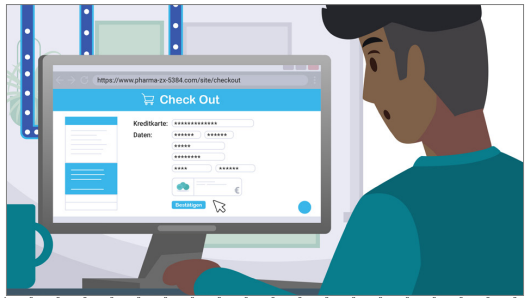
18



are then cheated out of their money on the fake store pages.

ANIMATION
Pharma page from image 9 suddenly appears (was redirected).

19



Paid goods are not shipped, personal data is tapped -

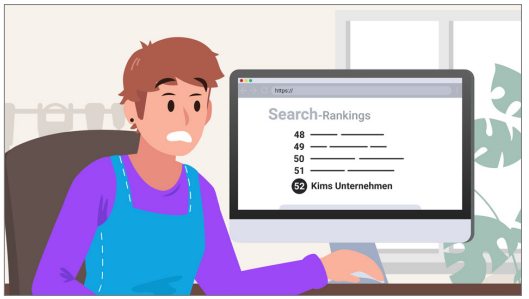
ANIMATION
Visitor makes a satisfied purchase on the site and enters his credit card number and his data (name, etc.). On the back of the monitor, this data is extracted through a clandestine digital connection.

20

or malicious malware is installed on visitors' computers.

ANIMATION
Visitor is startled when his/ her display is disturbed and a skull appears on it.

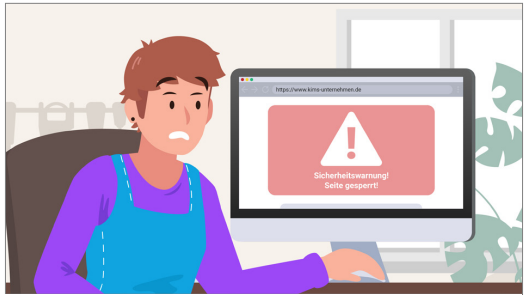
21



The hack is not without consequences for Kim either. The connection between Kim's site and the illegal fake shop ensures that Kim's painstakingly built-up rankings continue to deteriorate.

ANIMATION
Scene change to Kim. Kim looks at their monitor. The ranking of image 3 can be seen on it. Kim is no longer in 1st place. The ranking is scrolled down. Finally, their page appears at the very bottom. Kim looks startled.

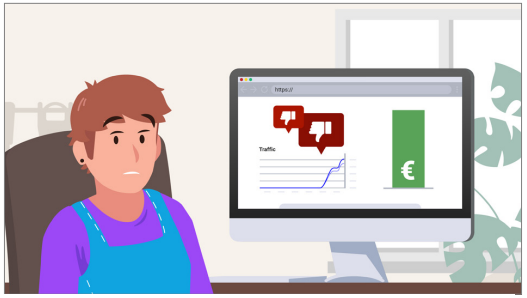
22



At worst, Kim's page is even classified as a security risk by the browser and can no longer be accessed at all.

ANIMATION
A window saying "Security warning! Website locked!" appears. Kim is horrified.

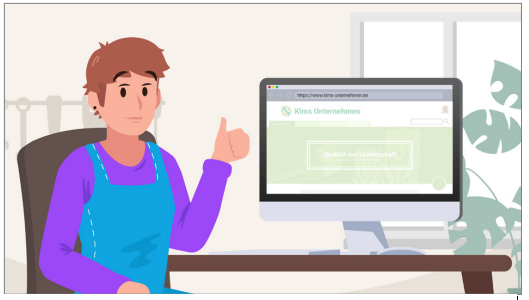
23



This means that the website hack causes Kim not only damage to their image, but also financial damage.

ANIMATION
Splitscreen on the monitor: On the left the increased traffic graph. Above appear thumbs-down. On the right a bar with a euro sign. The bar is dropping rapidly. Kim slides down in their chair, exhausted.

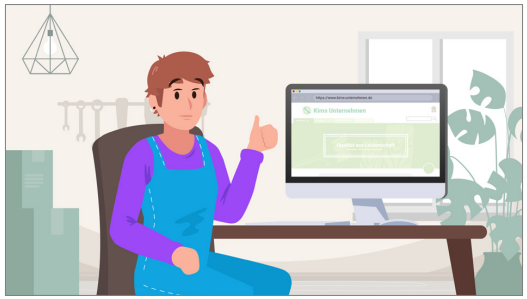
24



But: Recognizing that one's own website has been hacked is the first step in reducing such negative effects.

ANIMATION
Kim's monitor shows Kim's company website. Kim gives a thumbs-up.

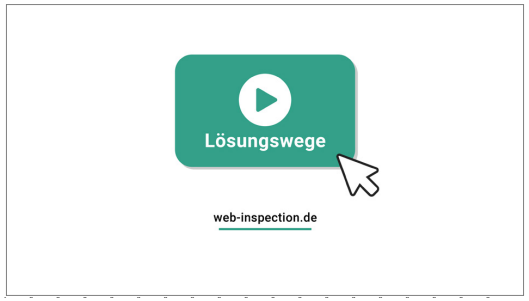
25



Would you like to find out more about website hacking and learn how you can best protect yourself?

ANIMATION
Slow zoom-out.

26



Then watch our second video or visit our website web-inspection.de.

ANIMATION
Video graphic appears. URL appears.

27

ANIMATION
Logos, contributors and sponsors appear.