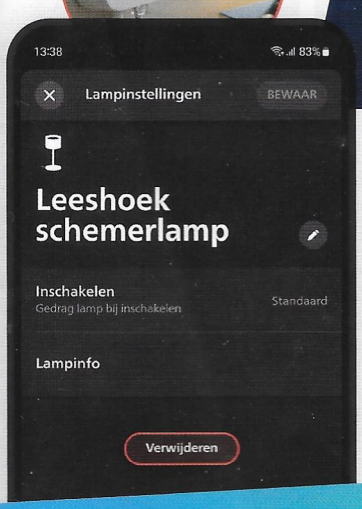
Computer idee 12

Workshops

Betere schermafdrukken in Windows 11

Filmische achtergronden op je eigen bureaublad



SLIM HUIS

Philips Hue zonder account



CHATGPT VS. GEMINI

Welke AI is het slimst?

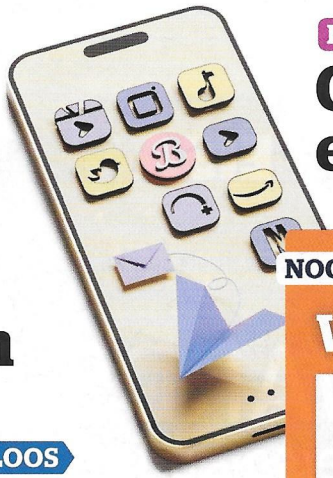
Smartphones gaan steeds langer mee!

Dankzij beter updatebeleid



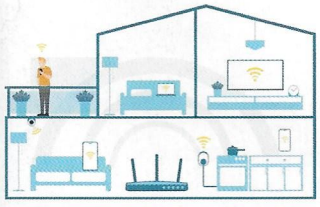
SLIMMER SCANNEN

Documenten en foto's digitaliseren



EIGEN ANDROID

Geef je smartphone een persoonlijk tintje



SNELLER DRAADLOOS

Wifi 7 komt, en dit heb je eraan

NOG JAREN VOORUIT

Windows 12 kan wachten!





Uitsmijter: Pas op voor op maat gemaakte phishing!

7 mei - 21 mei 2024 | € 5,75
RE SHIFT
BP
8 718226 104113 02412

Text Jolein de Rooij

Uitsmijter

Beware of tailored phishing!



During his PhD research, Pavlo Burda of Eindhoven University of Technology managed to get a disturbingly large number of people to fall for his phishing email.



PHOTO: VINCENT VAN DEN HOOGEN.

Who: Pavlo Burda
Where: Eindhoven
What: phishing
Why: to fight it

In the future, phishing will become even more convincing, says researcher Pavlo Burda of Eindhoven University of Technology (TU/e). That is because this form of fraud is becoming increasingly personal. How can you protect yourself against it?

How dangerous is phishing?

"With phishing, a criminal tries to get someone to do something foolish, such as sharing identity or login details, or installing malware. That can be the starting point for a whole range of attack techniques. These are not only used by criminals; companies also try to spy on or sabotage competitors this way. And states deploy phishing for electronic warfare, to break into foreign computer systems."

Why are we susceptible to it?

"It comes down to the way our brains work. We are good at thinking systematically and making decisions in a rational way, but that takes quite a lot of energy. Our brain can't keep that up all day. On top of that, it is slow. That is why we perform many actions on autopilot. If you are driving, for example, and the light turns green, you pull away almost without thinking. Unfortunately, scammers can also exploit our autopilot."

How do they exploit that?

"The American psychologist Robert Cialdini has written a great deal about this. For instance, we are particularly sensitive to authority. That makes us alert to all kinds of signals that point to it, from a police officer's uniform to the diplomas on the wall at a doctor's office. We also value reciprocity: when someone does something for us, we like to do something in return. That is exactly why restaurants give you free sweets with the bill. You then tip more and sooner. We are also sensitive to scarcity and time pressure. Companies play on this on Black Friday: the feeling that you'll miss out if you don't act fast. So there are all kinds of tricks you can use to persuade people to do something they weren't actually planning to do. These tricks are all aimed at switching off our common sense and making us switch over to autopilot."

Criminals switch off our reason?

"Yes, for example with a mix of time pressure and the threat of authority. An accountant, say, receives an email on a Friday afternoon, supposedly from the director, urging him to pay an invoice before the weekend. Another example: people have by now got used to paying by scanning a QR code. A few months ago, criminals in the US exploited that habit at a car park. They stuck a sticker on the parking meter, right over the existing QR code. That way, unsuspecting motorists transferred money into the criminals' own bank account. During my PhD research I mapped these kinds of mechanisms as precisely as possible, partly to be able to explain why one attack is more successful than another."

How did you research that?

"Among other things, our research group carried out a phishing experiment. In total, we sent around 750 people a phishing email, partly at TU/e and partly at a large Dutch consultancy firm. The latter organisation turned out to be more susceptible to phishing than my



In the phishing experiments Pavlo conducted, he lured people to a fake site where they had to enter their username and password. In reality, by the way, TU/e has been using multi-factor authentication for a few years now.

old university: thirty percent of the company's employees entered their username and password on a fake site, compared with ten percent of the university staff. Junior employees were also more susceptible to phishing emails that appeared to come from someone with authority within their organisation. At the consultancy, as many as 52 percent of them fell for it. But even more influential was the extent to which the email had been personalised. Was the person addressed by their own name? Was it about a topic that person was already familiar with? Was the email supposedly sent by someone from within the organisation?"

Is tailored phishing extra dangerous?

"Yes, and that is bad news. In the future we will probably receive a lot more of it. That is because people reveal a great deal of information about themselves on social media. Databases full of personal data also regularly end up out in the open. By combining all that data, you can build fairly detailed personal profiles. With those, you can tailor phishing to the individual, even automatically. Artificial intelligence offers additional possibilities for this. For example, I read about a 56-year-old woman from Enschede who, last year, thought she was getting a call from her son. He was panicking and said he had just caused a fatal accident. Only if he or his mother paid the funeral costs would he not be arrested. The mother was distraught and willing to do anything, until her son suddenly walked into the room. Then she realised the phone call was fake. The extortionists had cloned her son's voice."

How can we protect ourselves?

"Actually, we can't. We are all susceptible to phishing, you and I included. You can, however, make it harder to misuse stolen login details by setting up multi-factor authentication. In phishing attacks, reporting is also important. In one of my experiments, for example, some people saw through the phishing immediately and reported it straight away to their IT department. Those people are worth their weight in gold. And as an organisation, you need to make it easy to report phishing. After that, you have to respond quickly, because the damage grows with every hour. My research showed that after four hours, three quarters of the victims had already fallen for it."

What advice do you have for readers?

"It's better not to make your profiles on social networks such as Facebook, Instagram and LinkedIn publicly accessible, because there are software robots combing the entire internet in search of data. And if you have doubts about a message, don't respond from your phone. If possible, wait until you are back home and sitting calmly at your computer. By then you'll also have had more time to think the message over. Smartphones are very user-friendly, but on a large screen you see far more detail. That increases the chance that you'll recognise phishing."

Call-out

Doing something special with your computer? Or have you come up with a handy software solution for your hobby? Then send an email with the subject 'Rubriek Uitsmijter' to redactie@computeridee.nl
Who knows, you might end up in Computer Idee.

Sites

- www.pavlo.it
- www.kwikr.nl/nieuwetruc
- www.kwikr.nl/qrscam
- www.kwikr.nl/weaklink