Cultura Binaria

di **Michela Rovelli**

La lente adesiva che trasforma lo smartphone in microscopio

Se la fotocamera dello smartphone è ormai diventata una delle funzionalità più importanti per gli utenti — e quindi per le aziende produttrici che moltiplicano i sensori e li arricchiscono di intelligenza artificiale — c'è anche chi prova a sfruttarla per trasformare il dispositivo che tutti abbiamo in tasca in uno strumento «tecnico». Come il microscopio. Agli studenti e ai laboratori, ma anche ai fotografi professionisti (o amatoriali) è rivolta l'idea tutta italiana della startup SmartMicroOptics, nata all'interno dell'Istituto Italiano di Tecnologia e che è atterrata sulla piattaforma di crowdfunding Mamacrowd per raccogliere investimenti (c'è tempo fino al primo aprile). Per vedere il mondo in miniatura più nitido, basta applicare una delle quattro lenti adesive Blips create dalla startup sulla fotocamera di un telefono o di un tablet. Sono piccolissime, estremamente portatile e facili da mettere e togliere. Al 100 per cento prodotte in Italia.

Si può scegliere la lente giusta in base alle proprie esigenze. Per tutte, lo spessore si tiene al di sotto del millimetro. Dalle Blips Macro Plus, per ottenere immagini di piccoli insetti e fiori alle Blips Macro, con un ingrandimento ottico di dieci volte. Poi le Blips Micro, primo approccio al mondo della microscopia con riconoscimento di dettagli fino a 4,5 micron e infine le più sofisticate, le Blips Ultra, che riconosce anche particolari di 3,5 micron. Le più economiche? Costano 11,90 euro. «Nessun competitor è in grado di offrire una tale gamma di prodotti con questa fascia di prezzo», assicura il Ceo di SmartMicroOptics Andrea Antonini. In cantiere c'è già un nuovo kit chiamato Diple che trasforma lo smartphone in un vero strumento da laboratorio, in grado di analizzare anche globuli rossi e batteri.

PING CALLS E SNIFFING IL NUOVO VOCABOLARIO DELLA TRUFFA ONLINE

Una email su due nasconde un tentativo di frode (anche quando sembra certificata). Persino WhatsApp è a rischio
Dai Wi-Fi fake agli squilli «sconosciuti»: le contromisure per evitare le trappole della Banda Bassotti versione Internet

di **Antonino Caffo**

Inganni via mail
Molti cyber attacchi sfruttano la fiducia che riponiamo nella Pec, la posta certificata. Mentre gli account tradizionali sono sfruttati per inviare attacchi di phishing o link truffa

Sempre connessi e pronti a leggere messaggi e commenti, non ci accorgiamo di essere continuamente pedinati da hacker e criminali informatici. Quelle email periodiche che ci chiedono di inviare soldi al vecchio parente che ci ha lasciato un'eredità in Venezuela per sbloccarla, sono solo alcuni degli esempi di truffe che circolano in rete. Secondo gli ultimi dati dei Kaspersky Lab, la quota di *spam* nel traffico delle email nel 2018 è stata pari al 52,48% del totale, con un aumento del 4,15% rispetto al 2017. In pratica, un messaggio di posta ogni due ha rappresentato un tentativo di frode, con la Cina in cima ai paesi da cui lo *spam* proviene. I social network, gli hotspot wifi, le pubblicità sul web e persino WhatsApp possono diventare strumenti pericolosi se sfruttati come vettori di trasmissione di minacce.

Meglio evitare certe app e servizi? No di certo, ma tenere alta l'attenzione è quanto mai consigliato. Come ad esempio invita a fare il «Movimento difesa del cittadino» che da marzo del 2017 segue con attenzione il caso del raggiro in "alta definizione" su WhatsApp. Funziona così: un truffatore pubblica online varie inserzioni per la vendita di auto usate (ma potrebbe essere qualsiasi altro prodotto) e, una volta raggiunto l'accordo con l'acquirente, si fa inviare la foto di un assegno come impegno a concludere la trattativa. A quel punto, stampa l'immagine in alta definizione, nelle dimensioni di un vero assegno e, con l'appoggio di un contatto che si interpone con l'istituto bancario, riesce a incassare la cifra, senza più farsi vivo. Sembrerà banale ma proprio nell'era delle app e della digitalizzazione, colpi del genere vanno ancora in porto, peraltro senza che le vittime riescano poi a riottenere alcun risarcimento.

Basterebbe poco per difendersi da truffe simili, diffidando dall'invio di documenti sensibili via chat. Altro azzardo è quello di dar seguito a qualsiasi richiesta arrivi da un indirizzo PEC, la famosa posta certificata, o che si finge tale. L'aumento costante delle PEC ha infatti creato per migliaia di cyber criminali la possibilità di ottenere cospicui profitti. In che modo? L'utilizzo di questa forma di comunicazione garantisce al malintenzionato l'abbattimento della sfiducia che, per fortuna, molti hanno nell'aprire allegati o cliccare su link. Già nel 2017 la posta elettronica certificata è stata usata per diffondere virus a iosa e, nel 2018, il numero di PEC violate, arruolate poi inconsapevolmente per campagne hacker, è salito a oltre 500mila. Lo scorso maggio, centinaia di clienti di Banca Mediolanum, Banca Fineco, CheBanca!, Ing, IWBank e Barclays sono caduti nella trappola del «clicca qui per aggiornare i tuoi dati», di fatto consegnando il computer ai malware dei malfattori. Come difendersi? Andare oltre la semplice dicitura "PEC", che peraltro potrebbe benissimo essere confusa tra le righe e non ufficiale (antonio.rossi-PEC@gmail.com), evitando l'apertura di allegati misteriosi.

Quando l'hacker o il cracker, che lavora solo a scopo di lucro, non riesce a ingannare uno scaltro utente, resta possibile una modalità di intrusione non facile da individuare: il wifi *fake*. In giro per la città o nei pressi di luoghi di interesse si individuano spesso reti gratuite, che fanno molto comodo quando ci si trova all'estero o si è a corto di dati cellulare. Purtroppo, il *cyber crime* ha imparato a creare connessioni wireless aperte per attirare più persone possibile e intercettare i dati inviati attraverso il network. L'obiettivo? Nonostante le forme di protezione sempre più avanzate, come la verifica in due fattori che prevede l'inserimento di una password e di un codice temporaneo ricevuto via sms, ci sono ancora tante piattaforme il cui ingresso è