Unexpected Dangers for Small Businesses

Office recycling bins, USB drives, unwatched computers, social media profiles. Those are some of the possible weak spots hackers can use to harm small businesses. ESET cybersecurity expert Jake Moore regularly sets off into the field and investigates such hidden dangers that SMBs might not be aware of. Here are some of his experiences.

One man's trash is another man's treasure

Why should you care about what employees throw into office garbage bins? Because they might be putting valuable personal and company data at risk. "Millions of people throw sensitive information away every single day, and criminals are well aware of this," says Jake. Even parcel notes should be destroyed with a shredder, since they often include home addresses as well as email addresses and phone numbers.

Based on personal information, hackers can easily manipulate employees. "For example, with the phone number and the receipt of what a person just bought, they could potentially call or text an employee with an update on the purchased product. Also, they could ask him or her to visit phishing or other scam websites that could then entice the employee into handing over more information, such as passwords or payment card details," Jake adds. Eventually, cybercriminals might even access shopping accounts and purchase items from stored cards–including company ones.

When too much trust leads to cyberattacks

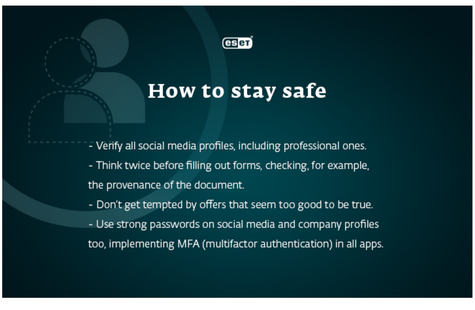
In August 2021, Jake, dressed as a TV assistant producer, visits a small but prominent UK golf club. The staff lets him in without questioning his identity or asking for an ID. He is left alone with most company devices. The staff even allows him to insert a USB stick into the devices, which were – to Jake's horror – still running on Windows XP. Just like that, within mere minutes, Jake gains access to the whole company network. "With access to the Wi-Fi password, USB ports and even unsupervised machines, I could have completed any exploit I could dream up, from installing a remote access trojan or keyloggers onto the machines, to placing other malware, such as ransomware, on the network to demand payment to decrypt the data." A real hacker's delight.

Read more in the interview with Jake.

HackedIn via LinkedIn

If you want to network professionally, having a LinkedIn profile is almost a must.But as much as you care about your online presentation, you should also care about cybersecurity. **Social networks might become another potential threat** and are a great channel for cybercriminals. One example that says it all: While working as a security consultant, Jake tried to coax crucial personal data out of the CEO of a small company in Dorset, and LinkedIn was his first choice. He created a fake profile and sent a request to the personal assistant of the CEO, which he immediately accepted.

Without really verifying the profile's identity, the assistant started communicating with Jake and agreed to shoot a spot about the company. Next, Jake sent a believable questionnaire, asking for the personal details of the CEO, which the head of the company willingly filled in. Afterward, the assistant forwarded all the materials to Jake. And just like that, Jake (who could have been a hacker) was provided crucial security information, which could easily be misused.



The more we're online, the more digital touchpoints appear. Cybercriminals leverage their skills to get into your business, and they bet on their target's **naivete, truthfulness or politeness**. Nevertheless, within the digital environment, more than anywhere else, it is always necessary to look before you leap – or click, in this case.