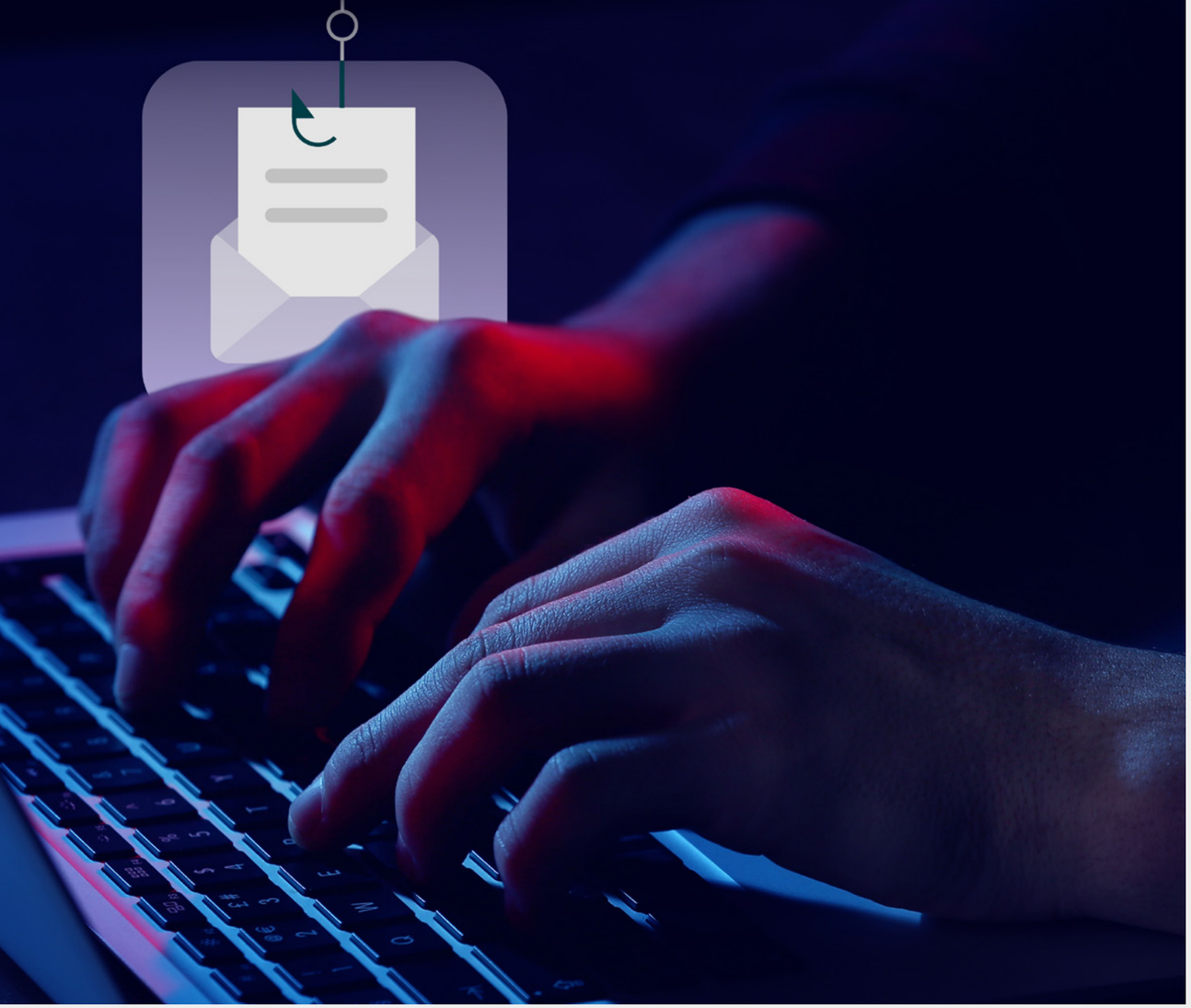
sosafe

Top 5 Cybercrime Trends 2022

Latest Trends in Cybercrime and
How Your Organization Can Stay Safe



01 Trendy phishing: topical attacks

Cybercriminals are still using one common tool: Manipulating victims' emotions in order to obtain and exploit confidential information in different ways. To do this, they remain updated on current affairs and latest societal developments. Furthermore, their phishing emails often provoke fear and uncertainty, which pressures victims to click on harmful content and end up paying ransom or handing over personal information.

The attackers are unscrupulous when it comes to the events and issues that they use in their phishing messages. The coronavirus pandemic was a prime opportunity: Just a few weeks after the COVID-19 Omicron variant became global news, one phishing attempt in the United Kingdom took advantage of this crisis.[1] Russia's attack on Ukraine also resulted in an unprecedented rise in cybercrime, especially phishing. For example, fraudulent charity fundraisers were disseminated on social media and through phishing emails.[2] In one particularly malicious scheme, links were shared that allegedly supported DDoS attacks to disrupt Russian servers and services. When recipients clicked on the links, cybercriminals got access to infect their systems with viruses and Trojans.[3] At the same time, Google's research team reported phishing attacks against Eastern European states and US-based NGOs carried out by Russian hacking groups. Here, too, the attackers were targeting confidential access credentials for espionage or the spread of malware.[4] Phishing is therefore becoming a digital weapon in hybrid warfare.

In combination with the possibilities offered by modern technology (see trend 4), organizations all over the world are facing a new generation of highly innovative and destructive phishing attacks. Artificial intelligence is playing a key role in making these far more precise, personalized, and thus more successful.

Practical tip

Cybercriminals use phishing to emotionally manipulate their victims. The best way to protect your organization is to reduce uncertainty by teaching your employees about these tactics so that they will not cave under pressure, fear, or curiosity after receiving fraudulent emails. Provide cyber security awareness training that contains the latest information (including new attack methods) and phishing simulations that cover a wide range of attack scenarios. This way you can help your employees recognize and ward off phishing emails, no matter how topical and duplicitous they may seem.

1 The Independent (2021). Scam warning over fake omicron testing text messages.
2 Zeit Online (2022). Wie können wir helfen?
3 SoSafe (2022). SoSafe warns of social engineering attacks in the context of the war of aggression against Ukraine.
4 ZDNet (2022). Google: Multiple hacking groups are using the war in Ukraine as a lure in phishing attempts.

02 Supply chain attacks: explosive chain reactions

The number of supply chain attacks increased by 51 percent in 2021,[5] and this trend is continuing in 2022. The reason: Cybercriminals are improving their chances of success via their victims' partner and supplier networks. In some circumstances, security flaws in the supply chain (in the software used by a partner or supplier, for example) are all it takes to compromise the entire network. The consequences of this can be devastating and far-reaching.

Groups like Revil, BlackMatter, and DarkSide recently conducted large-scale attacks against the HR platform Kronos, the oil pipeline system Colonial Pipeline, and the meat producer JBS. Chinese cyber espionage group APT27, also known as LuckyMouse or EmissaryPanda, has also increasingly targeted companies with information theft and cyberespionage campaigns. The critical sector, including organizations in the pharmaceutical and tech industries, was also compromised through their supply chains.[6]

The ransomware attack on IT service provider Kaseya is a striking example of the damage that these complex methods can cause: The perpetrators used a fake software update to access Kaseya's servers. The infected software infiltrated the IT systems of its customers and compromised the entire supply chain. This "software supply chain attack" affected between 800 and 1,500 companies worldwide.[7] The Log4J vulnerability that was discovered in December 2021 can also be attributed to these software supply chain attacks, which illustrates the complexity and long-term impact that these incidents can have.[8]

5 TechRepublic (2022). Supply chain cyberattacks jumped 51% in 2021.
6 Bleeping Computer (2022). German government warns of APT27 hackers backdooring business networks.
7 The Washington Post (2021). Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack.
8 Forrester (2021). Log4j, Open Source Maintenance, Andy Why SBOMs Are Critical Now.
9 Gartner (2021). The Top 8 Cybersecurity Predictions for 2021-2022.

Practical tip

In addition to strengthening your organization's security culture, you should also select partners that have strong information and data security systems. If your network of partners has suitable security mechanisms in place, there is a lower risk of your organization falling victim to a supply chain attack. For example, (software) certifications or fulfillment of regulations like the EU GDPR can be assessed and ensured. According to Gartner, 60 percent of all organizations believe cyber security risks will play a major role in conducting business deals and evaluation of potential partners by 2025.[9]

03 Multiple extortion: compound attacks increase risk of damage

The European Union Agency for Cybersecurity (ENISA) says that we are in a "golden age of ransomware," and not without reason. The number of attacks with extortion schemes in 2021 more than doubled compared to 2020.[10] This is an attack method in which cybercriminals secretly install malware on company systems and encrypt sensitive data, which they hold against ransom. To do this, they try to access the systems either via the human factor (e.g., phishing emails) or by using technical methods like brute force to fish for data. Both methods are becoming increasingly successful, and attacks with massive extortion sums have made international headlines in 2022.

One-time extortion and purely technical attacks have thus become a thing of the past. Cybercriminals now use sophisticated attacks that utilize psychological tactics in their extortion and compound them with other attacks. This is known as multiple extortion: Cybercriminals follow up their initial theft, encryption, and ransom of sensitive data (with the threat of releasing these data if the ransom isn't paid) with other methods such as DDoS attacks, crypto mining, or bot networks. Attackers can use DDoS attacks to overload or block their victims' websites until their demands are met.

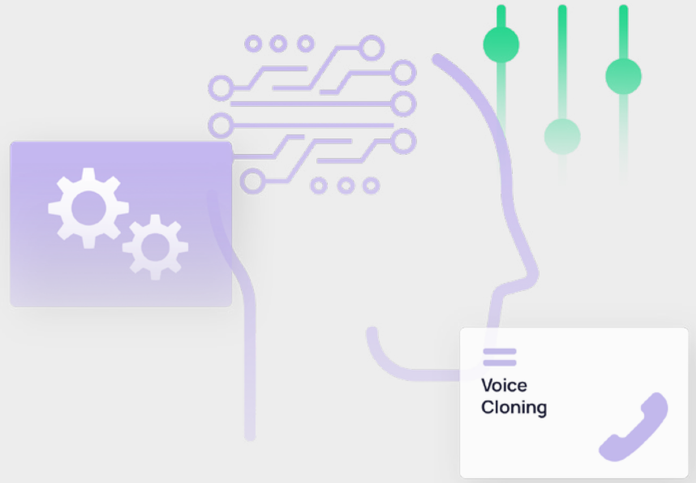
In April 2021, ransomware group REvil attacked computer manufacturer Quanta. When the company did not meet the ransom demands, the attackers tried the same tactic with Apple – a client of Quanta Computer – and threatened to publish stolen data on the latest MacBook Pro. It is unclear whether Apple paid the $50 million USD ransom.[11] In mid-2022 the group ALPHV/Black Cat attacked a luxury spa in the United States and then released the personal information of over 4,000 customers in a searchable format.

[10] European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.
[11] Bloomberg (2021). Apple Targeted in $50 Million Ransomware Hack of Supplier Quanta.
[12] Krebs on Security (2022). Ransomware Group Debuts Searchable Victim Data.

The information could then be publicly viewed on a website – an insidious way to compel the victims to pay a ransom themselves.[12] Not only do organizations have to pay to reactivate their systems in addition to the ransom itself, but they often must grapple with irreparable harm to their reputation.

Practical tip

Cybercriminals' tactics are always evolving. You should keep your security systems updated to protect your digital infrastructure against attacks. This includes creating regular backups. Your training content should also always be adapted to current and industry-specific threats. The human factor is often the first target, even with ransomware attacks – and usually in the form of a phishing email. Strengthen your security culture and make sure that you have an incident response plan in place so that you can minimize the damage.



04 Deepfakes: harmless fun or dangerous deception?

Artificial intelligence (AI) has become a household term due to the arrival of voice assistants like Siri and Alexa, smart automation tools, and smart homes. However, cybercriminals also quickly realized that this technology can be used for social engineering attacks like phishing, as they are a prime opportunity to maximize profits.

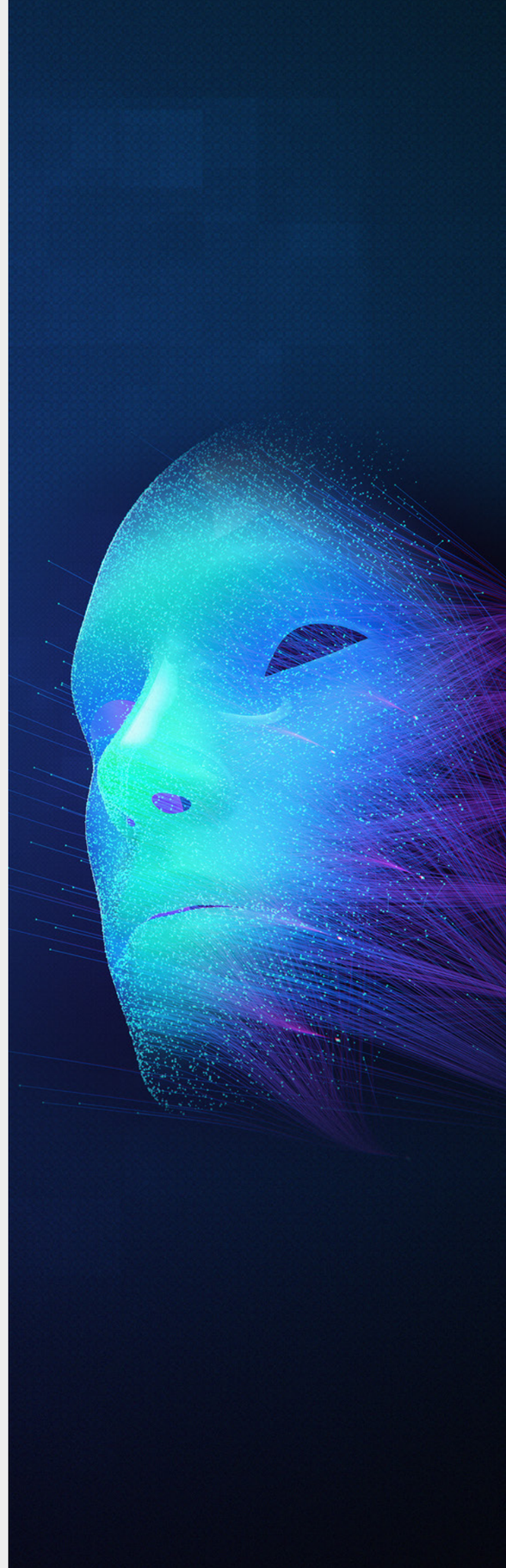
Voice phishing (vishing) is already being successfully combined with deepfake technology to make phishing emails appear more legitimate. In a tactic known as "voice cloning", the attackers imitate the voice of a supervisor to lure employees to disclose sensitive information or transfer funds. In 2020, criminals were able to steal $35 million USD from a bank in Hong Kong this way.[13]

As the quality of deepfakes increases and the effort to create them decreases, cybercriminals are sure to conduct more believable and successful attacks in the future. This is best exemplified by the many examples in pop culture and FaceApp, which lets anyone create fake audio-video content. It becomes difficult for the naked eye to differentiate between many deepfakes and their authentic counterparts.

Cyberattacks that use deepfake technology have also caused turmoil. For example, Mayor Franziska Giffey of Berlin was recently contacted by an AI-based Vitali Klitschko to discuss the war in Ukraine via video conference. Soon thereafter it was discovered that this was nothing more than a "cheapfake", in which manipulated audio material is dubbed over existing video material. This attack illustrated how deepfakes can lead to dangerous disinformation and manipulation.[14]

Practical tip

Although a number of research groups are currently working on developing an AI-based screening tool for detecting deepfakes, purely technical measures don't hold up in the fight against this ever-evolving technology. And because they are so widespread in pop culture, deepfakes are usually considered to be harmless. Therefore, you can use AI-assisted security measures and raise awareness of these risks. It is important to give your staff the tools they need to correctly identify and report potentially harmful content.



[13] Forbes (2021). Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find.

[14] DW (2022). Vitali Klitschko fake tricks Berlin mayor in video call.

05 Hybrid working: putting your employees in charge of cyber security

The number of organizations that rely on hybrid work has risen sharply since the COVID-19 pandemic began. This also leaves them more vulnerable to cyberattacks. 75 percent of the respondents polled for the Human Risk Review 2022 confirm that the risk landscape has worsened as a result of hybrid working models.

There are a number of reasons for this:

- **Lack of technical security**

  Only just over half of Americans (61%) use a VPN connection at work.[15]

- **New means of attack**

  Collaboration tools like Microsoft Teams and cell phones, which are used more frequently in remote work settings, offer new targets.

- **Uncertainty**

  Employees exhausted by the pandemic and remote work are more prone to ignore security protocols and best practices.[16]

The successful ransomware attack on Colonial Pipeline in April 2021 showed the type of consequences hybrid work can have: Cybercriminals got their hands on a password that was not used securely, giving them remote access to an employee's VPN account as well as many internal systems and data. This resulted in widespread gasoline shortage on the East Coast of the United States.[17]

Practical tip

When your employees move into a hybrid work model, you are giving them most of the control over your systems' information security. Make sure that your team knows how to handle this responsibility. Provide your employees with robust training that corresponds to their personal work situation. Context-based training measures such as personalized phishing simulations minimize the risk of falling victim to cyberattacks.

15 Statista (2021). Virtual private network (VPN) usage in the United States from 2019 to 2021, by location.

16 ZDNet (2021). Everyone is burned out. That's becoming a security nightmare.

17 Bloomberg (2021). Hackers Breached Colonial Pipeline Using Compromised Password.

The Human Risk Review 2022

Learn more about cybercrime trends and the current cyberthreat landscape in the Human Risk Review 2022.

Learn more →

About SoSafe

SoSafe empowers organizations to build a security culture and mitigate risk with its GDPR-compliant awareness platform. Powered by behavioral science and smart algorithms, SoSafe delivers engaging personalized learning experiences and smart attack simulations that turn employees into active assets against online threats. Comprehensive analytics measure ROI and tell organizations where vulnerabilities lie. The platform is easy to deploy and scale, fostering secure behaviour in every employee.

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Germany

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800