Cybercrime, AI and the growing need for digital identity protection

The protection of our digital identity is becoming more and more crucial as phishing activity remains high and AI provides increased opportunities for criminals. Malicious online activity is still on the rise, and we stress the high importance of using safe mobile phones. Mobile safety features could also be of interest to telecom operators

Source: The development of AI is just one of many factors adding yet another layer of complexity to the mix when it comes to tackling cybercrime

Phishing activity remains high

Many of us have received an email with the false promise of an inheritance of a deceased (unknown) family member, a business proposal that was too good to be true. The aim of these emails is to engage in a conversation while revealing confidential information in the process.

This is one of the most disturbing forms of cybercrime – the theft of personally identifiable information, or phishing. This data allows further criminal practices that could lead to great (financial) damage. Today, scammers approach us through all available communication channels, including those on mobile phones.

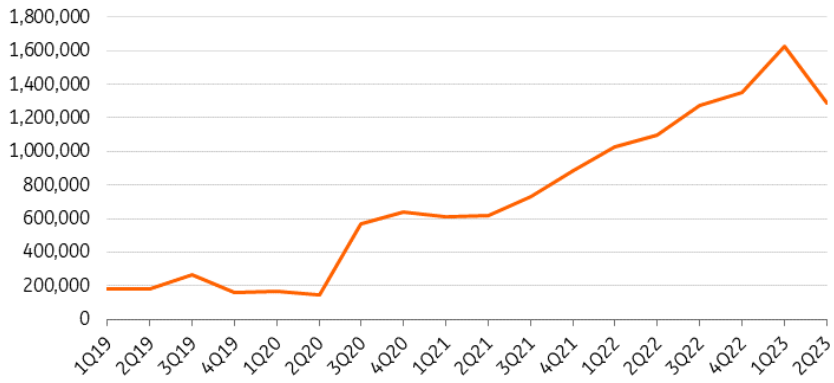
Throughout the years, phishing activity has seen a strong increase, despite a slowdown during the

second quarter of 2023. The increase in phishing activity is the result of increasing professional capabilities. Nevertheless, it could be that the second quarter data reflects international law enforcement agencies finding some success in taking down the large criminal trading website Genesis Market through Operation Cookiemonster. But also the malware from Qakbot has been taken down and the ransomware group HIVE.

Today, many employees and customers are trained to recognise phishing attempts, and there is now software available that monitors and blocks traffic that is directed towards phishing sites. Even so, we expect that activity will pick up going forward because criminal networks are likely to continue improving their professional skills. Opportunities will also increase as the number of devices that can be used for phishing rises. Notably, towards the end of 2023, low-tech phishing attempts were on the rise, luring customers to scan QR codes that directed them to malicious sites.

Phishing activity went up significantly throughout the years

Number of unique phishing Web sites (attacks) detected



APWG, ING

AI may help criminals

Some criminals engaging in cybercrime can be highly sophisticated – but equally, others are often just testing the waters and giving things a try. Often, these could be spotted through spelling mistakes. AI may unfortunately increase the risk that comes from less sophisticated fortune seekers. AI technology provides an easy way to produce well-written messages and can help with impersonating others through manipulated audio messages or with training criminals. Criminals committing cybercrimes have also professionalised in recent years, with organised groups now providing services for each step along the value chain. Fortunately, companies may also benefit from AI helping to analyse and detect traffic with malicious intent.

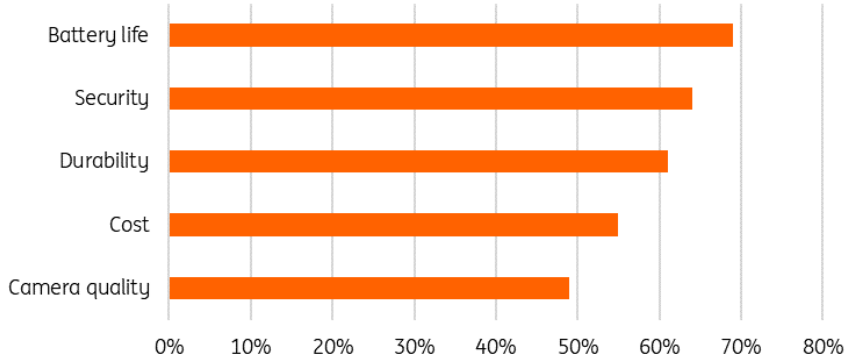
Identity data theft continues to pose a challenge

As a result of the increasing threat, defences against unauthorised access and data theft have to be in place. These measures involve additional layers of protection against social engineering, but also against malicious software. In the context of the 2024 Telecom Outlook, we identify three trends evolving around the need for secure and trusted data connections. We see a greater need for multi-factor authentication, a bigger demand for secure connections (VPNs), as well as a greater acceptance of endpoint protection software. These measures obviously have to be taken

into wider security policies and a secure infrastructure, based on the concept that requests to access information and systems can only be trusted unless it is verified (zero trust infrastructure).

Smartphone purchasing criteria

Security ranks second as very important reason to choose the next smartphone



Source: GSMA Intelligence, ING

Mobile phones take centre stage in efforts to enhance digital safety

As research by the GSMA shows, security risks rank in the top three most considered features for buying a mobile phone, right after battery life. Apple is a company that sees safety as a key feature, and this differentiates the brand from others. It operates a trusted ecosystem, limiting the ability of users to install software that was not checked for its safety aspects. Today, there is greater pressure on phone manufacturers to make security-enhancing software updates available for a considerable period, as shown by new standards such as the Protection Profile for securing smartphones from the ETSI. Legacy phones with an outdated and unsafe operating system expose their users to phishing attacks and privacy infringements. Surprisingly, we do not see much business communication encouraging people to replace old phones with new ones for their improved safety features. The same holds true for the use of software enhancing mobile safety. While software protecting the network endpoints (such as the phone) is very common in a business environment, this is not the case for consumers.

As most of us know, mobile phones can also be used as a means to provide an additional layer of security. There are many identification apps, such as Microsoft Authenticator or Google Authenticator, which enable multi-factor authorisation. But phones also offer the infrastructure through which a verification code can be sent. This is done through providers such as Twilio, CM.COM and Telesign (part of the telecom company Proximus). These tools greatly help to improve access security for digital infrastructure. They can also act as a building block for interesting business offerings that are around. Nevertheless, once a device (such as a mobile phone) is unsafe, authentication from that device becomes unreliable. This shows again why devices need to be safe and protected.

Telecom providers could enhance their role, enhancing digital safety

We think safety-enhancing features offer a further opportunity for telecom operators, although they already do a lot to protect digital infrastructure today. Telecom operators could further seduce customers to replace unsafe phones, while consumers may start to use software that enhances the safety of mobile phones (end-point protection software) and look for services that protect their identity and data integrity (VPN software).

Vodafone and KPN are among the companies that are leading the way here. Vodafone offers security software for mobile phones in the business segment, while KPN has a collaboration with ESET, a global digital security company. Traditionally, cyber defence efforts were directed towards the business segments and telecom operators already have offerings in place for this market segment. A notable example is Orange. Orange has been growing its cyber defence entity by 14% year-on-year in 2022 to €977mln and 11.4% YoY in the first half of 2023. The objective is to generate €1.3bn of revenues from cybersecurity services in 2025. This clearly shows that there are opportunities in the telecom space.

Author

Jan Frederik Slijkerman
Senior Sector Strategist, TMT
jan.frederik.slijkerman@ing.com

Diederik Stadig
Sector Economist, TMT & Healthcare
diederik.stadig@ing.com

Additional information is available on request. For more information about ING Group, please visit www.ing.com.