Dariya Protasova, Elena Mazko
Science tutor *L. Bedritskaya*
BSEU (Minsk)

HOW TO PROTECT YOUR ORGANIZATION AGAINST PHISHING ATTACKS?

The purpose of our paper is to show that protection against phishing attacks is very relevant at the moment and to give some advice on how to protect your company from them.

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message [1].

These are 5 of the most common types of phishing attacks:

1. Deceptive Phishing

Deceptive phishing is by far the most common type of phishing scam. In this ploy, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials.

2. Spear Phishing

In this type of ploy, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender.

3. CEO Fraud

Spear phishers can target anyone in an organization, even executives. That's the logic behind a "whaling" attack. In these scams, fraudsters try to harpoon an exec and steal their login details.

4. Vishing

This type of phishing attack dispenses with sending out an email and instead goes for placing a phone call. An attacker can perpetrate a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds

5. Smishing

This method leverages malicious text messages to trick users into clicking on a malicious link or handing over personal information using a phone [2].

Here are some outrageous phishing stats showing the severity of the situation:

1. 97% of the users are unable to recognize a sophisticated phishing email.
2. Only 3% of the users report phishing emails to the management.
3. 30% of phishing emails are opened by users, and 12% of these targeted users click on the malicious link or attachment.
4. 85% of all organizations have been hit by a phishing attack at least once.
5. The creation of around 1.5 million new phishing sites is witnessed every month.
6. 1 in every 8 employees shares information on a phishing site.

7. 1 in every 2 organizations has been targeted by a ransomware attack in 2019 and data was successfully encrypted by the attackers in 73% of these attacks [3] [4].

As mentioned above, phishing is a threat that is equally likely to appear on a desktop computer, laptop, or smartphone. Therefore, we have formulated some of the most important rules that will help your employees not to fall for the hook of scammers:

1. Educate Employees About Current Phishing Threats

Phishing attacks use human nature to trick people into doing something that the attacker wants. Common techniques include creating a sense of urgency and offering the recipient of the email something that they desire, which increases the probability that the target will take action without properly validating the email.

2. Teach Employees to Report Suspicious Emails

Most phishing attacks don't target a single employee within a company. Instead, an attacker will send a number of emails. For this reason, it is important to train employees to report any emails that they suspect may be phishing attacks. Even if one employee doesn't fall for the phish, another might.

3. Inform Employees About Corporate Email Policies

Every organization should have an email security policy, including anti-phishing principles defining acceptable use of email. This policy should describe acceptable and unacceptable use and how to respond to potential attacks.

4. Review Password Security Best Practices

User credentials are one of the primary targets of cybercriminals. If an attacker has an employee's password, it can be much more difficult to detect ongoing attacks since they can masquerade as a legitimate user. Additionally, employees commonly use the same password for multiple online accounts, meaning that a single breached password can grant an attacker access to a number of the employee's online accounts. It is important to educate employees about the threat posed by phishing emails and about password security best practices. These include the need to use unique, strong passwords for all of their accounts, to never share passwords, and to never enter a password into a page reached by a link that was sent via email.

5. Deploy an Automated Anti-Phishing Solution

While phishing education can help to reduce the number of successful phishing attacks against the organization, some emails are likely to sneak through. Minimizing the risk of phishing attacks to the organization requires AI-based anti-phishing software capable of identifying and blocking phishing content across all of the organization's communication services (email, productivity applications, etc.) and platforms (employee workstations, mobile devices, etc.).

REFERENCES:

1. Phishing attacks [Electronic resource]. – Mode of access: imperva.com/learn/phishing-attack. – Date of access: 11.03.2021.

2. 5 Common Phishing Attacks [Electronic resource]. – Mode of access: www.tripwire.com/state-of-security/security-awareness/5-common-phishing-attacks-and-how-to-protect-against-them. – Date of access: 12.03.2021.

3. 2020 Phishing statistics [Electronic resource]. – Mode of access: www.keepnetlabs.com/phishing-statistics-you-need-to-know-to-protect-your-organization. – Date of access: 10.03.2021.
4. Staggering Phishing Statistics in 2020 [Electronic resource]. – Mode of access: https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020. – Date of access: 10.03.2021.

Polina Makaruk
Science tutor *N. Potapova*
BSTU (Brest)

NEW SKILLS OF THE ACCOUNTANT PROFESSION IN THE DIGITAL ECONOMY

Technological progress is clearly changing our world, and the pace of such changes is constantly increasing. This applies to all aspects of life and work. Professions change, disappear and emerge in a completely new form. The emergence of the digital economy and digital society are global trends of the modern era that are becoming part of the global ecosystem.

The formation of the digital economy has raised the issue of digital skills for the accounting profession, since the transition to Industry 4.0 significantly changes the labor market: along with the spread of information technology in all spheres of life, digital skills are becoming critically important from the point of view of employers. The fourth industrial revolution is characterized by widespread digitalization, blurring the lines between the physical, digital and biological spheres. The ongoing changes are at the intersection of several trends, but nevertheless, key attention is paid to the automation of production and management processes [1].

The purpose of the study is to identify the main directions of the formation of key skills of a professional accountant in the digital economy.

In the next 20-30 years, a large-scale transformation of the requirements for professional accountants is expected, since many operations that were not previously affected by digital technologies will be automated in the near future or will disappear due to a change in the way accounting is organized. The use of new technologies in accounting directly affects the speed and quality of transactions, reduces the influence of the human factor and, accordingly, reduces their number. The use of artificial intelligence makes it possible to optimize and automate accounting processes.

The new economy will require a new type of specialists. They will face challenges that will require creativity and a willingness to collaborate with others and with artificial intelligence systems. The very approach to accounting work will change.

Key skills of the digital economy are interpreted as competencies that are necessary for an employee to solve a given task or achieve a given result of activity in the context of global digitalization of social and business processes. Thus, the digital