Hindawi
Security and Communication Networks
Volume 2021, Article ID 3394325, 8 pages
https://doi.org/10.1155/2021/3394325

Research Article

An Incentive Mechanism for Reporting Phishing E-Mails Based on the Tripartite Evolutionary Game Model

Mengli Wang[1] **and Lipeng Song**[2]

[1]*Data Science and Technology, North University of China, Taiyuan 030051, China*
[2]*School of Mechanical, Electrical & Information Engineering, Shandong University, Weihai 264209, China*

Correspondence should be addressed to Lipeng Song; slp880@gmail.com

Received 23 April 2021; Accepted 9 June 2021; Published 18 June 2021

Academic Editor: Zhenhua Tan

The human is considered as the important link in the phishing attack, and the e-mail security provider encourages users to report suspicious e-mails. However, evidence suggests that reporting is scarce. Therefore, we study how to motivate users to report phishing e-mails in this paper. To solve the problem, a tripartite evolutionary game model among e-mail security providers, e-mail users, and attackers is constructed. We obtain the desired evolutionary stable strategy through solving the replicator dynamics equations. Moreover, the evolution process to the desired evolutionary stable strategy is derived, which can guide the e-mail security provider to make a reasonable incentive mechanism. Lastly, we experiment with a large real-world e-mail network. The experiment results show that our model is effective and practical.

1. Introduction

While e-mail is widely used as an efficient communication tool on the Internet, users are plagued by spam and phishing e-mails. According to the report by Kaspersky Lab, the share of such unwanted e-mails in e-mail traffic amounted to 50.37% in 2020 [1]. The spam wastes user's time and misuses valuable network resources. Even worse, phishing e-mails can steal personal confidential information and compromise government systems and companies spanning every economic sector [2, 3]. FBI estimated that phishing e-mails caused over $1.8 billion financial loss in 2020 [4]. Therefore, it is important to protect e-mail users from phishing e-mails.

Since phishing e-mails aim at exploiting human weakness, effective mitigation would require addressing issues at the technical and human layers [5, 6]. In the technical layer, machine learning is the main approach to detecting phishing e-mails [2, 7, 8]. However, attackers may bypass detection techniques. Besides, users are the most vulnerable link in the phishing ecosystem [9]. Therefore, users play an important role in preventing phishing attacks. Today, the most widely implemented user-focused intervention is to train individuals to increase their security awareness [10–13]. Major training methods emphasize reporting; they encourage users to report suspicious e-mails to e-mail security providers [14]. This is because that reporting makes early detection possible and allows e-mail security providers to inform other potential victims before the attack spreads. To make reporting easy, e-mail security providers have provided a convenient mechanism (e.g., Cofense Reporter [15]). Though there are many benefits of reporting phishing e--mails, most users do not choose to report phishing e-mails [16–18].

Prior research explained why users do not report phishing e-mails based on Social Cognitive Theory [14]. However, it does not provide an effective incentive mechanism. In this paper, we study how to encourage users to report phishing e-mails? An e-mail security provider (ESP), such as Gmail, is responsible to protect their paying users from phishing e-mails. In other words, ESP should formulate a reasonable incentive scheme to encourage users. We adopt the game theory to analyze the important factors affecting user behavior from the perspective of players' expected benefits. Meanwhile, each player cannot obtain all

the information to make the optimal decision in the actual situation. In other words, they are all bounded rationality [19, 20]. Therefore, we adopt the evolutionary game theory that satisfies this premise. The main contributions of this paper are summarized as follows:

(i) We construct a tripartite evolutionary game model among e-mail security providers, e-mail users, and attackers. Then, we obtain an expected evolutionary stable strategy, which is all users choose to report suspicious e-mails, all attackers do not send phishing e-mails, and all e-mail security providers choose to check reported e-mails. Moreover, we derive an evolution process that can guide the e-mail security provider to reach the desired stable state.

(ii) To validate the model, we experiment with a large real-world e-mail network. The experiment results show that our model is effective in the real-world e-mail network.

(iii) We explore the influence of the attack punishment on the evolution path by numerical simulation. The simulation results show that increasing attack punishment has a great influence on the rate at which attackers evolve toward nonattacking.

The remainder of this paper is organized as follows. In Section 2, an evolutionary game model including e-mail security providers, e-mail users, and phishing attackers is proposed. Section 3 constructs the replicator dynamics equations and obtains the evolutionary stability strategy and its evolution process. In Section 4, we explore the influence of the network topology, the attack punishment, and the user payoff on the evolution path. Section 5 summarizes the whole paper.

2. Evolutionary Game Model

In this section, we define the strategies and payoffs of the game players.

2.1. Problem Statement. The problem consists of three game groups: e-mail security providers, e-mail users, and phishing attackers. The e-mail security provider aims to protect paying users from phishing e-mails with the least cost and increase the number of paying users. The e-mail user aims to obtain a secure e-mail experience with minimal cost. The goal of an attacker is to send phishing e-mails to steal personal information with the minimum risk of being detected by the defender. We assume that the game groups have bounded rationality.

2.2. Analysis of Strategies. In the tripartite evolutionary game model, the e-mail security provider has two alternative strategies: supervision and nonsupervision. On the one hand, ESP can choose supervision, which needs to deploy additional security personnel and equipment to check and store the reported e-mails. While supervision incurs additional cost, it will improve the ESP's reputation and thus increase the number of paying users. On the other hand, ESP can choose to ignore reported e-mails to reduce the corresponding management cost. However, in the long run, some negative reputation effects will be generated and the number of paying users may decrease.

Attackers have two alternative strategies: attacking and nonattacking. When an attacker sends out phishing e-mails, he may successfully trick users or not. Whether an attack succeeds or not depends on the user behavior. We assume the probability of successfully attacking is one, which equivalently reduces the attack cost. Because this paper mainly studies the strategy of the e-mail user, and the attacker can be simplified. After the attacker sends phishing e-mails, he may be reported by users or not. If he is reported, he will be punished by the ESP selecting supervision.

E-mail users have two alternative strategies: reporting and nonreporting. After receiving an e-mail, the user will check whether the e-mail is a phishing e-mail. When the e-mail is suspected to be a phishing e-mail, the user may report it or not. If the user chooses to report a suspicious e-mail, the reported e-mail may be a phishing e-mail or not. In other words, the user may correctly report a phishing e-mail or not. The user will be rewarded by the ESP choosing supervision if he correctly reports a phishing e-mail. If the user falsely reports an e-mail, he will not be held accountable because of the service principle. Moreover, he will receive feedback from the ESP choosing supervision and thus avoid missing important e-mails. However, no matter which choice e-mail users make, a phishing e-mail will cause losses to e-mail users, including the losses of money and time.

2.3. Payoff Matrix and Expected Benefit. The tripartite payoff matrix is shown in Table 1. a_i, b_i, and c_i, respectively, represent the payoff of users, attackers, and ESPs in the corresponding strategy. Suppose that the proportion of users selecting reporting is x; then, the proportion selecting nonreporting is $1 - x$. Suppose also that the proportion of attackers selecting attacking is y, and the proportion selecting nonattacking is $1 - y$. The proportion of ESPs selecting supervision is z, and the proportion selecting nonsupervision is $1 - z$. Obviously, $0 \le x \le 1$, $0 \le y \le 1$, and $0 \le z \le 1$.

Because the payoff of each game group will be affected by the strategies of the other two game groups, there are eight combinations of strategies for users, attackers, and ESPs: (reporting, attacking, and supervision), (reporting, nonattacking, and supervision), (nonreporting, attacking, and supervision), (nonreporting, nonattacking, and supervision), (reporting, attacking, and nonsupervision), (reporting, nonattacking, and nonsupervision), (nonreporting, attacking, and nonsupervision), and (nonreporting, nonattacking, and nonsupervision). The payoff of each combination is shown in equations (1)–(8). The parameters and their meanings are shown in Table 2, and all parameter values are not less than zero:

Table 1: The tripartite payoff matrix

E-mail user	x		$1-x$	
Attacker	y	$1-y$	y	$1-y$
ESP z	(a_1, b_1, c_1)	(a_2, b_2, c_2)	(a_3, b_3, c_3)	(a_4, b_4, c_4)
ESP $1-z$	(a_5, b_5, c_5)	(a_6, b_6, c_6)	(a_7, b_7, c_7)	(a_8, b_8, c_8)

Table 2: Model parameters and meanings.

Parameters	Meanings
G_{u1}	User's reward received from the ESP selecting supervision for correctly reporting a phishing e-mail
G_{u2}	User's payoff when he falsely reports an e-mail and the ESP gives him feedback on the e-mail
C_{u1}	User's cost for reporting a suspicious e-mail, such as time cost
C_{u2}	User's loss caused by a phishing e-mail, such as personal information disclosure
G_a	Attack gain, namely, attack payoff minus attack cost
C_{a1}	Attack loss caused by the ESP selecting supervision when the phishing e-mail is reported
G_d	ESP's reputation improvement brought by supervision, which can be qualified by the number of paying users
C_{d1}	ESP's supervision cost, such as manager cost and storage cost
C_{d2}	ESP's reward cost for users correctly reporting a phishing e-mail

$$(a_1, b_1, c_1) = (G_{u1} - C_{u1} - C_{u2}, G_a - C_{a1}, G_d - C_{d1} - C_{d2}), \tag{1}$$

$$(a_2, b_2, c_2) = (G_{u2} - C_{u1}, 0, G_d - C_{d1}), \tag{2}$$

$$(a_3, b_3, c_3) = (-C_{u2}, G_a, -C_{d1}), \tag{3}$$

$$(a_4, b_4, c_4) = (0, 0, -C_{d1}), \tag{4}$$

$$(a_5, b_5, c_5) = (-C_{u1} - C_{u2}, G_a, -G_d), \tag{5}$$

$$(a_6, b_6, c_6) = (-C_{u1}, 0, 0), \tag{6}$$

$$(a_7, b_7, c_7) = (-C_{u2}, G_a, -G_d), \tag{7}$$

$$(a_8, b_8, c_8) = (0, 0, 0). \tag{8}$$

As shown in equations (9)–(11), U_{A1} represents the expected benefit of users adopting reporting, U_{A2} represents the expected benefit of users adopting nonreporting, and $\overline{U}_A$ represents the expected benefit of users:

$$\begin{aligned} U_{A1} = {} & yza_1 + (1-y)za_2 + y(1-z)a_5 \\ & + (1-y)(1-z)a_6, \end{aligned} \tag{9}$$

$$\begin{aligned} U_{A2} = {} & yza_3 + (1-y)za_4 + y(1-z)a_7 \\ & + (1-y)(1-z)a_8, \end{aligned} \tag{10}$$

$$\begin{aligned} \overline{U}_A = {} & xyza_1 + x(1-y)za_2 + xy(1-z)a_5 \\ & + x(1-y)(1-z)a_6 + (1-x)yza_3 \\ & + (1-x)(1-y)za_4 + (1-x)y(1-z)a_7 \\ & + (1-x)(1-y)(1-z)a_8. \end{aligned} \tag{11}$$

As shown in equations (12)–(14), U_{B1} represents the expected benefit of attackers adopting attacking, U_{B2} represents the expected benefit of attackers adopting nonattacking, and $\overline{U}_B$ indicates the expected benefit of attackers:

$$U_{B1} = xzb_1 + (1-x)zb_3 + x(1-z)b_5 + (1-x)(1-z)b_7, \tag{12}$$

$$U_{B2} = xzb_2 + (1-x)zb_4 + x(1-z)b_6 + (1-x)(1-z)b_8, \tag{13}$$

$$\begin{aligned} \overline{U}_B = {} & xyzb_1 + (1-x)yzb_3 + xy(1-z)b_5 \\ & + (1-x)y(1-z)b_7 \\ & + x(1-y)zb_2 + (1-x)(1-y)zb_4 \\ & + x(1-y)(1-z)b_6 + (1-x)(1-y)(1-z)b_8. \end{aligned} \tag{14}$$

Similarly, U_{C1} represents the expected benefit of ESPs employing supervision, U_{C2} represents the expected benefit of ESPs employing nonsupervision, and $\overline{U}_C$ indicates the expected benefit of ESPs, as shown in the following equation:

$$\begin{aligned} U_{C1} &= xyc_1 + (1-x)yc_3 + x(1-y)c_2 + (1-x)(1-y)c_4, \\ U_{C2} &= xyc_5 + (1-x)yc_7 + x(1-y)c_6 + (1-x)(1-y)c_8, \\ \overline{U}_C &= xyzc_1 + (1-x)yzc_3 + x(1-y)zc_2 \\ &\quad + (1-x)(1-y)zc_4 \\ &\quad + xy(1-z)c_5 + (1-x)y(1-z)c_7 \\ &\quad + x(1-y)(1-z)c_6 + (1-x)(1-y)(1-z)c_8. \end{aligned} \tag{15}$$

3. Equilibrium Analysis of the Evolutionary Game Model

In this part, we construct replicator dynamics equations. By analyzing the Jacobian matrix, we obtain evolutionary stable strategies and their evolution process.

3.1. Replicator Dynamics. The replicator dynamics equation of users is shown in the following equation:

$$\begin{aligned} F(x) &= \frac{\mathrm{d}x}{\mathrm{d}t} \\ &= x\left(U_{A1} - \overline{U}_A\right) \\ &= x(1-x)\left(U_{A1} - U_{A2}\right) \\ &= x(1-x)\left[yz\left(G_{u1} - G_{u2}\right) + zG_{u2} - C_{u1}\right]. \end{aligned} \tag{16}$$

The replicator dynamics equation of attackers is shown in the following equation:

$$\begin{aligned} G(y) &= \frac{\mathrm{d}y}{\mathrm{d}t} \\ &= y\left(U_{B1} - \overline{U}_B\right) \\ &= y(1-y)\left(U_{B1} - U_{B2}\right) \\ &= y(1-y)\left(-xzC_{a1} + G_a\right). \end{aligned} \tag{17}$$

The replicator dynamics equation of ESPs is shown in the following equation:

$$\begin{aligned} H(z) &= \frac{\mathrm{d}z}{\mathrm{d}t} \\ &= z\left(U_{C1} - \overline{U}_C\right) \\ &= (1-z)\left(U_{C1} - U_{C2}\right) \\ &= z(1-z)\left[xy\left(G_d - C_{d2}\right) + xG_d + yG_d - C_{d1}\right]. \end{aligned} \tag{18}$$

3.2. Equilibrium Solutions and Stability Analysis. To get the equilibrium solution of the above model, a replicator dynamics equation set is required, as shown in the following equation:

$$\begin{cases} F(x) = x(1-x)\left[yz\left(G_{u1} - G_{u2}\right) + zG_{u2} - C_{u1}\right] \\ = 0, \\ G(y) = \ y(1-y)\left(-xzC_{a1} + G_a\right) \\ = 0, \\ H(z) = z(1-z)\left[xy\left(G_d - C_{d2}\right) + xG_d + yG_d - C_{d1}\right] \\ = 0. \end{cases} \tag{19}$$

In (19), there are eight pure-strategy equilibrium points E_1 (0, 0, 0), E_2 (0, 0, 1), E_3 (0, 1, 0), E_4 (1, 0, 0), E_5 (1, 1, 0), E_6 (1, 0, 1), E_7 (0, 1, 1), and E_8 (1, 1, 1). In general, there exists a mix-strategy equilibrium point E_9 (x^*, y^*, z^*). According to Selten [21] and Ritzberger and Wainwright [22], if and only if a strategy combination is a pure-strategy Nash equilibrium, it will be asymptotically stable in the dynamic replication system of the tripartite evolutionary game. Moreover, the asymptotically stable equilibrium point must be the evolutionary stable strategy (ESS). Thus, the ESS must be a pure-strategy Nash equilibrium [23]. Hence, E_9 is not an evolutionary stable strategy because it is a mix strategy. In the following part, we analyze the asymptotic stability of the other eight equilibrium points. The Jacobian matrix of the tripartite evolutionary game is as follows:

$$\begin{aligned} J_1 &= \begin{bmatrix} \dfrac{\partial \mathrm{F(x)}}{\partial x} & \dfrac{\partial \mathrm{F(x)}}{\partial y} & \dfrac{\partial \mathrm{F(x)}}{\partial z} \\ \dfrac{\partial \mathrm{G(y)}}{\partial x} & \dfrac{\partial \mathrm{G(y)}}{\partial y} & \dfrac{\partial \mathrm{G(y)}}{\partial z} \\ \dfrac{\partial \mathrm{H(z)}}{\partial x} & \dfrac{\partial \mathrm{H(z)}}{\partial y} & \dfrac{\partial \mathrm{H(z)}}{\partial z} \end{bmatrix}, \\ &= \begin{bmatrix} J_{11} & J_{12} & J_{13} \\ J_{21} & J_{22} & J_{23} \\ J_{31} & J_{32} & J_{33} \end{bmatrix}, \end{aligned}$$

$$\begin{aligned} J_{11} &= (1-2x)\left[yz\left(G_{u1} - G_{u2}\right) + zG_{u2} - C_{u1}\right], \\ J_{12} &= x(1-x)\left[z\left(G_{u1} - G_{u2}\right)\right], \\ J_{13} &= x(1-x)\left[y\left(G_{u1} - G_{u2}\right) + G_{u2}\right], \\ J_{21} &= y(1-y)\left(-zC_{a1}\right), \\ J_{22} &= (1-2y)\left(-xzC_{a1} + G_a\right), \\ J_{23} &= y(1-y)\left(-xC_{a1}\right), \\ J_{31} &= z(1-z)\left[y\left(G_d - C_{d2}\right) + G_d\right], \\ J_{32} &= z(1-z)\left[x\left(G_d - C_{d2}\right) + G_d\right], \\ J_{33} &= (1-2z)\left[xy\left(G_d - C_{d2}\right) + xG_d + yG_d - C_{d1}\right]. \end{aligned} \tag{20}$$

According to Lyapunov [24], a point is an evolutionary stable strategy if and only if all eigenvalues of the Jacobian matrix corresponding to the point are negative. The eigenvalues can be obtained by solving the Jacobian matrix, and then, the asymptotic stability of each point is analyzed. As shown in Table 3, E_3 (0, 1, 0), E_6 (1, 0, 1), E_7 (0, 1, 1), and E_8 (1, 1, 1) have the possibility to be the ESS, and the remaining four equilibrium points are saddle points.

The strategies represented by E_3 (0, 1, 0) are that users do not report suspicious e-mails, attackers send phishing e--mails, and ESPs do not supervise reported e-mails. The prerequisite for E_3 (0, 1, 0) to be the ESS is $G_d - C_{d1} < 0$, that is, the reputation positive effects generated by supervision are less than the supervision cost.

The strategies represented by E_6 (1, 0, 1) are that users report suspicious e-mails, attackers do not send phishing e-mails, and ESPs supervise reported e-mails. The prerequisite for E_6 (1, 0, 1) to be the ESS is

Table 3: The stability analysis of the equilibrium points.

Equilibrium point	Eigenvalues of Jacobin matrix	Stability conditions
E_1 (0, 0, 0)	$\lambda_1 = -C_{u1}$ $\lambda_2 = G_a$ $\lambda_3 = -C_{d1}$	The equilibrium point is the saddle point because $G_a > 0$
E_2 (0, 0, 1)	$\lambda_1 = G_{u2} - C_{u1}$ $\lambda_2 = G_a$ $\lambda_3 = C_{d1}$	The equilibrium point is the saddle point because $G_a > 0$ and $C_{d1} > 0$
E_3 (0, 1, 0)	$\lambda_1 = -C_{u1}$ $\lambda_2 = -G_a$ $\lambda_3 = G_d - C_{d1}$	The equilibrium point is ESS, if $G_d - C_{d1} < 0$; otherwise, it is a saddle point
E_4 (1, 0, 0)	$\lambda_1 = C_{u1}$ $\lambda_2 = G_a$ $\lambda_3 = G_d - C_{d1}$	The equilibrium point is the saddle point because $G_a > 0$ and $C_{u1} > 0$
E_5 (1, 1, 0)	$\lambda_1 = C_{u1}$ $\lambda_2 = -G_a$ $\lambda_3 = 3G_d - C_{d1} - C_{d2}$	The equilibrium point is the saddle point because $C_{u1} > 0$
E_6 (1, 0, 1)	$\lambda_1 = C_{u1} - G_{u2}$ $\lambda_2 = G_a - C_{a1}$ $\lambda_3 = C_{d1} - G_d$	The equilibrium point is ESS, if $C_{u1} < G_{u2}, G_a < C_{a1}$, and $C_{d1} < G_d$; otherwise, it is a saddle point
E_7 (0, 1, 1)	$\lambda_1 = G_{u1} - C_{u1}$ $\lambda_2 = -G_a$ $\lambda_3 = C_{d1} - G_d$	The equilibrium point is ESS, if $G_{u1} < C_{u1}$ and $C_{d1} < G_d$; otherwise, it is a saddle point
E_8 (1, 1, 1)	$\lambda_1 = C_{u1} - G_{u1}$ $\lambda_2 = C_{a1} - G_a$ $\lambda_3 = C_{d1} + C_{d2} - 3G_d$	The equilibrium point is ESS, if $C_{u1} < G_{u1}, C_{a1} < G_a$, and $C_{d1} + C_{d2} < 3G_d$; otherwise, it is a saddle point

$C_{u1} < G_{u2}$, $G_a < C_{a1}$, and $C_{d1} < G_d$, that is, the reporting cost is less than the user's payoff for falsely reporting an e-mail, the attack gain is less than the attack loss, and the reputation positive effects generated by supervision are greater than the supervision costs. This prerequisite can prompt the ESP to implement supervision and eventually enable attackers and users to evolve into nonattacking and reporting. The equilibrium point is the final stable state expected by this paper.

The strategies represented by E_7 (0, 1, 1) are that users do not report suspicious e-mails, attackers send phishing e--mails, and ESPs supervise reported e-mails. The prerequisite for E_7 (0, 1, 1) to be the ESS is $G_{u1} < C_{u1}$ and $C_{d1} < G_d$, that is, the reporting reward from ESP is less than the report cost, and the reputation positive effects generated by supervision are greater than the supervision cost.

The strategies represented by E_8 (1, 1, 1) are that users report suspicious e-mails, attackers send phishing e-mails, and ESPs supervise reported e-mails. The prerequisite for E_8 (1, 1, 1) to be the ESS is $C_{u1} < G_{u1}$, $C_{a1} < G_a$, and $C_{d1} + C_{d2} < 3G_d$, that is, the reporting reward from ESP is greater than the report cost, the attack gain is greater than attack loss, and the reputation positive effects generated by supervision are greater than a third of the supervision costs plus reward cost.

As shown in Figure 1, the evolution process is E_3 (0, 1, 0)$\longrightarrow E_7$(0, 1, 1)$\longrightarrow E_8$ (1, 1, 1)$\longrightarrow E_6$ (1, 0, 1).

E_3 (0, 1, 0) is the initial state, namely, nonreporting, attacking, and nonsupervision. All ESPs choose supervision

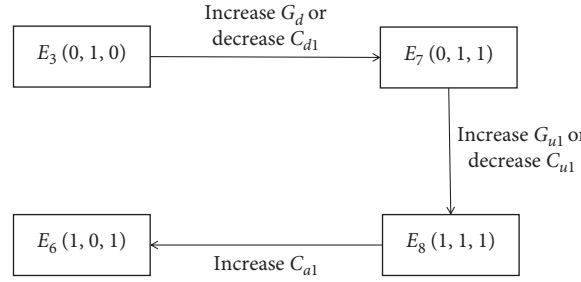

Figure 1: : Evolution process of ESS.

if $C_{d1} < G_d$. Therefore, the state E_3 (0, 1, 0) will be converted to E_7 (0, 1, 1) if the positive reputation effect is more than the supervision cost. The state E_7 (0, 1, 1) will be converted to E_8 (1, 1, 1) if $G_{u1} > C_{u1}$, that is, the reporting reward is more than the reporting cost. Therefore, in this stage, the ESP should increase the reporting reward G_{u1} or decrease the reporting cost C_{u1}. Lastly, the state E_8 (1, 1, 1) will be converted to E_6 (1, 0, 1) if $G_a < C_{a1}$, that is, the attack loss is more than the attack gain. Therefore, in this stage, the ESP should increase attack punishment strength.

4. Numerical Simulation

In this part, we first verify that our model is effective in the real-world e-mail network. Then, we explore the influence of two important parameters on the evolution path.

4.1. Numerical Simulation of Network Topology. The replicator dynamic equation assumes that e-mail users are evenly mixed, that is, the user can learn from each other. However, in practice, the e-mail user learns from his neighbourhood. Therefore, we experiment with a large real-world e-mail network. The e-mail network dataset was collected in North University of China from September 2016 to March 2018 and includes 452 e-mail users and more than 10000 edges. The initial parameters are set as follows: $G_{u1} = 10$, $G_{u2} = 2$, $C_{u1} = 1$, $C_{u2} = 3$, $G_a = 1$, $C_{a1} = 10$, $G_d = 15$, $C_{d1} = 5$, and $C_{d2} = 10$. Besides, to objectively evaluate the evolution path of players, we start from a neutral point. In other words, we set the initial proportions of users, attackers, and ESPs as 0.5. We simulated with the above parameters for 1000 times. Figure 2 shows the evolution paths of users, attackers, and ESPs in an evenly mixed e-mail network. Figure 3 shows the evolution paths of users, attackers, and ESPs in the real-world e-mail network. The results show that the network structure of e-mail users has little influence on the evolution path. Thus, our model is practical and effective.

4.2. Numerical Simulation of Variable Parameters. Among all the parameters, there are two important parameters in the model: the user payoff for falsely reporting an e-mail G_{u2} and the attacker loss when the phishing e-mail is reported to ESP adopting supervision C_{a1}. In this part, the influences of the two parameters on the evolution paths of participants will be studied. In practice, the user group is neutral, the attacker group prefers to send phishing e-mails to get gain, and the ESP prefers to nonsupervision to reduce the corresponding management cost. Thus, in the following simulations, we set the initial proportion of users selecting reporting, attackers sending phishing e-mails, ESP selecting supervision as 0.5, 0.9, and 0.1, respectively.

In this paragraph, we study the influence of G_{u2} on the evolution path. We set $G_{u1} = 4$, $C_{u1} = 1$, $C_{u2} = 3$, $G_a = 1$, $C_{a1} = 2$, $G_d = 15$, $C_{d1} = 5$, and $C_{d2} = 4$, keeping other parameters and the initial proportions of players unchanged. As shown in Figure 4, the convergence rate of e-mail users and attackers is accelerated as G_{u2} increases. G_{u2} is the user payoff for falsely reporting an e-mail to the ESP selecting supervision. On the one hand, the reported e-mail is more important; G_{u2} will increase. On the other hand, the feedback from ESP is sooner, and G_{u2} is larger. Therefore, increasing the feedback speed can accelerate the convergence speed of users and attackers. Moreover, a suspicious e-mail is more important; the user is more willing to report the e-mail.

In this paragraph, we study the influence of C_{a1} on the evolution path. We set $G_{u1} = 4$, $G_{u2} = 2$, $C_{u1} = 1$, $C_{u2} = 3$, $G_a = 1$, $G_d = 15$, $C_{d1} = 5$, and $C_{d2} = 4$, keeping other parameters and the initial proportions of players unchanged. As shown in Figure 5, the convergence rate of attackers is

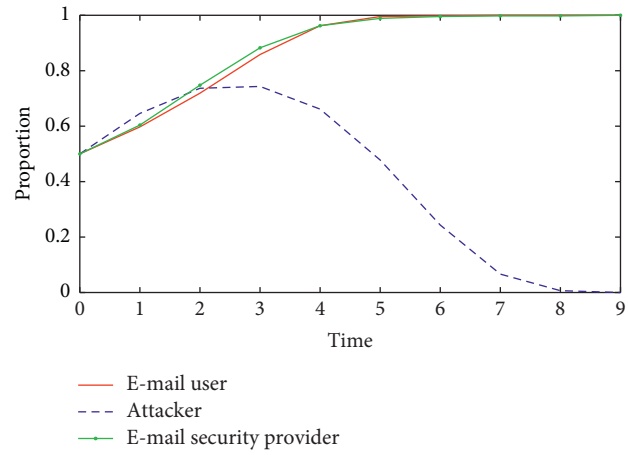

Figure 2: The evolution path with evenly mixed users.

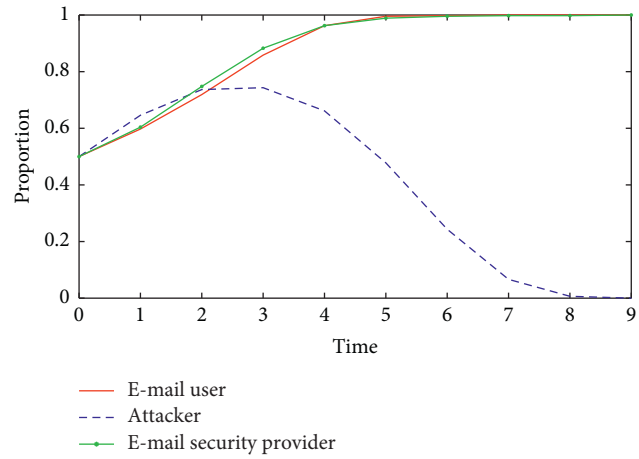

Figure 3: The evolution path in a real-world e-mail network.

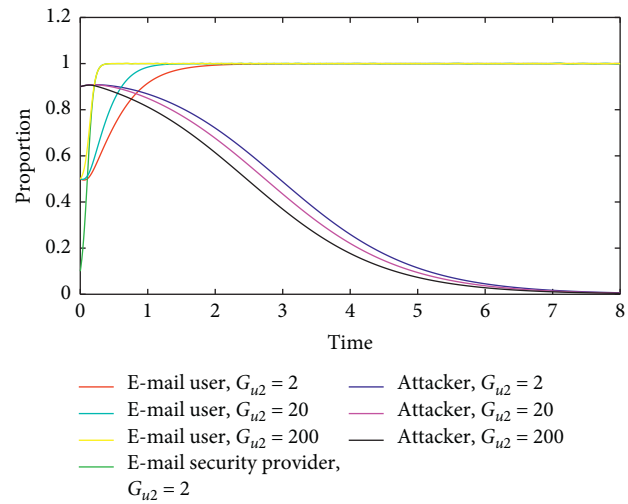

Figure 4: The evolution paths with different values of G_{u2}.

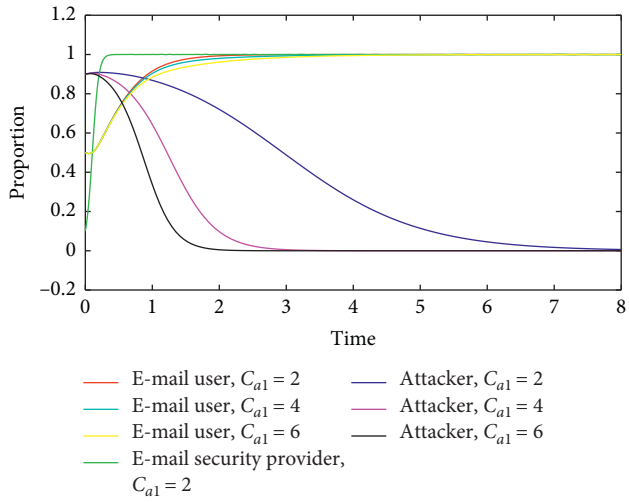

Figure 5: The evolution paths with different values of C_{a1}.

accelerated as C_{a1} increases. Therefore, the ESP should increase attack punishment strength.

5. Conclusions

The main goal of this paper is to mitigate phishing e-mails from the human layer. As the human is considered as the important link in the phishing attack, the e-mail security provider can reduce the phishing attack through cooperating with e-mail users. Therefore, we construct a tripartite evolutionary game model, which considers the payoffs of e-mail security providers, e-mail users, and attackers. Through analyzing the eigenvalues of the Jacobian matrix corresponding to each equilibrium point, we obtain four possible evolutionary stable strategies. Moreover, we obtain the evolution process of the four evolutionary stable strategies, which can guide the e-mail security provider to make a reasonable mechanism to reach the desired state. Finally, we verify that our model is effective in a real-world e-mail network.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 61772478).

References

[1] Kaspersky. Spam and phishing in 2020 n.d. 2020, https://securelist.com/spam-and-phishing-in-2020/100512/.

[2] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," *Artificial Intelligence Review*, vol. 53, no. 7, pp. 5019–5081, 2020.

[3] G. Ho, A. Cidon, L. Gavish et al., "Detecting and characterizing lateral phishing at scale," in *Proceedings of the 28th USENIX Security Symposium*, pp. 1273–1290, USENIX Association, Santa Clara, CA, USA, August 2019.

[4] Federal Bureau of Investigation, "Internet crime report. 2021," Federal Bureau of Investigation, Washington, DC, USA, 2020.

[5] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013.

[6] G. Park, L. M. Stuart, J. M. Taylor, and V. Raskin, "Comparing machine and human ability to detect phishing emails," in *Proceedings of the 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 8–13, IEEE, San Diego, CA, USA, October 2014.

[7] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, vol. 67, no. 2, pp. 247–267, 2018.

[8] C. Sur, "Ensemble one-vs-all learning technique with emphatic & rehearsal training for phishing email classification using psychology," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 30, no. 6, pp. 733–762, 2018.

[9] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, "SoK: a comprehensive reexamination of phishing research from the security perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 671–708, 2020.

[10] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, "Why do some people manage phishing e-mails better than others?" *Information Management & Computer Security*, vol. 20, no. 1, pp. 18–28, 2012.

[11] P. Kumaraguru, Y. Rhee, A. Acquisti, L. Cranor, and E. N. Jason Hong, "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," in *Proceedings of the 2007 Conference on Human Factors in Computing Systems, CHI 2007*, pp. 187–193, Springer Berlin Heidelberg, San Jose, California, USA, April 2007.

[12] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails," *Online Information Review*, vol. 40, no. 2, pp. 265–281, 2016.

[13] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: exploring embedded training and awareness," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 28–38, 2014.

[14] Y. Kwak, S. Lee, A. Damiano, and A. Vishwanath, "Why do users not report spear phishing emails?" *Telematics and Informatics*, vol. 48, Article ID 101343, 2020.

[15] Cofense. The Easiest Way to Report Phishing n.D, 2021, https://cofense.com/product-services/reporter/.

[16] Swinhoe D., Why Businesses Don't Report Cybercrimes to Law Enforcement 2019, https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

[17] https://www.verizon.com/business/resources/reports/dbir/ Verizon. 2020 Data breach investigations report. 2020.

[18] N. Stembert, A. Padmos, M. S. Bargh, S. Choenni, and F. Jansen, "A study of preventing email (spear) phishing by enabling human intelligence," in *Proceedings of the 2015 European Intelligence and Security Informatics Conference*, pp. 113–120, IEEE, Manchester, UK, September 2015.

[19] L. Vinet and A. Zhedanov, "A "missing" family of classical orthogonal polynomials," *Journal of Chemical Information and Modeling*, vol. 53, pp. 1689–1699, 2010.
[20] D. Pu, F. Xie, and G. Yuan, "Active supervision strategies of online ride-hailing based on the tripartite evolutionary game model," *IEEE Access*, vol. 8, Article ID 149052, 2020.
[21] R. Selten, "A note on evolutionarily stable strategies in asymmetric animal conflicts," *Journal of Theoretical Biology*, vol. 84, no. 1, pp. 93–101, 1980.
[22] K. Ritzberger and J. W. Weibull, "Evolutionary selection in normal-form games," *Econometrica*, vol. 63, no. 6, pp. 1371–1399, 1995.
[23] C. G. Hewitt and J. Wainwright, "A dynamical systems approach to Bianchi cosmologies: orthogonal models of class B," *Classical and Quantum Gravity*, vol. 10, no. 1, pp. 99–124, 1993.
[24] A. M. Lyapunov, "The general problem of motion stability," *Annals of Mathematics Studies*, vol. 17, pp. 203–474, 1992.