This is an illustration of a phishing scheme. According to the Federal Trade Commission, a phishing scheme is defined as, “A type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. It asks the consumer to provide personal identifying information.” Essentially what this means is that the attackers have built a phony website that appears to be identical to the actual one. This attack is particularly disturbing since the attackers were able to convince the employees that the email was legitimate, and they voluntarily gave sensitive information. To avoid a repeat of this incident, it is vital that all employees receive regular security awareness training.

Phishing emails and SMS messages frequently present a tale to persuade you to click on a link or open an attachment. You may get an unexpected email or text message that appears to be from a firm you know or trust, such as a bank, credit card, or utility provider. It might also be from an online payment website or app.

**The communication might have come from a fraudster who may claim a few (or all) of the following examples within their email:**

* say they’ve noticed some suspicious activity or log-in attempts — they haven’t
* claim there’s a problem with your account or your payment information — there isn’t
* say you need to confirm some personal or financial information — you don’t
* include an invoice you don’t recognize — it’s fake
* want you to click on a link to make a payment — but the link has malware
* say you’re eligible to register for a government refund — it’s a scam
* offer a coupon for free stuff — it’s not real

(<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>)

The first step after finding out that a phishing scheme has been initiated within your work environment would be to launch an investigation to determine the scale of the attack, identify any compromised systems or data, and gather evidence for any potential legal action. It would also be vital to notify those who have been affected and provide information on how to protect themselves from potential identity theft or fraud.

**The signs of an email being a phishing scheme could include the following:**

* The email has a generic greeting.
* The email says your account is on hold because of a billing problem.
* The email invites you to click on a link to update your payment details.

(<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams> )

To avoid a repetition of this situation, it is vital that all employees receive regular security awareness training to ensure they understand the risks of phishing efforts and how to recognize them. To prevent employees from visiting phony websites or getting phishing emails, email filters, web filters, and DNS filtering should be enabled. Frequent vulnerability assessments and penetration testing are also suggested to detect and remedy any faults in the systems that attackers may exploit. To respond quickly and effectively to any security events, an incident response strategy must be in place.

**A few preventative measures that can be used for this type of training might include the following:**

1. Use security software to protect your PC. Configure the program to automatically update so that it can cope with any new security concerns.

2. Safeguard your phone by configuring the software to automatically update. These upgrades may provide you with vital security protection.

3. Use multi-factor authentication to secure your accounts. Some accounts provide additional protection by needing two or more credentials to log in. This is referred to as multi-factor authentication. Multi-factor authentication makes it more difficult for scammers to access your accounts if they have your login and password.

4. Back up your data to protect it. Back up your computer's data to an external hard drive or the cloud. Back up your phone's data as well.

**Works Cited:**<https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams>

<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

This is an illustration of a phishing scheme. According to the Federal Trade Commission, a phishing scheme is defined as, “A type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. It asks the consumer to provide personal identifying information.” Essentially what this means is that the attackers have built a phony website that appears to be identical to the actual one. This attack is particularly disturbing since the attackers were able to convince the employees that the email was legitimate, and they voluntarily gave sensitive information. To avoid a repeat of this incident, all employees must receive regular security awareness training.

Phishing emails and SMS messages frequently present a tale to persuade you to click on a link or open an attachment. You may get an unexpected email or text message that appears to be from a firm you know or trusts, such as a bank, credit card, or utility provider. It might also be from an online payment website or app.

**The communication might have come from a fraudster who may claim a few (or all) of the following examples within their email:**

* say they’ve noticed some suspicious activity or log-in attempts — they haven’t
* claim there’s a problem with your account or your payment information — there isn’t
* say you need to confirm some personal or financial information — you don’t
* include an invoice you don’t recognize — it’s fake
* want you to click on a link to make a payment — but the link has malware
* say you’re eligible to register for a government refund — it’s a scam
* offer a coupon for free stuff — it’s not real

(<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>)

The first step after finding out that a phishing scheme has been initiated within your work environment would be to launch an investigation to determine the scale of the attack, identify any compromised systems or data, and gather evidence for any potential legal action. It would also be vital to notify those who have been affected and provide information on how to protect themselves from potential identity theft or fraud.

**The signs of an email being a phishing scheme could include the following:**

* The email has a generic greeting.
* The email says your account is on hold because of a billing problem.
* The email invites you to click on a link to update your payment details.

(<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams> )

To avoid a repetition of this situation, all employees must receive regular security awareness training to ensure they understand the risks of phishing efforts and how to recognize them. To prevent employees from visiting phony websites or getting phishing emails, email filters, web filters, and DNS filtering should be enabled. Frequent vulnerability assessments and penetration testing are also suggested to detect and remedy any faults in the systems that attackers may exploit. To respond quickly and effectively to any security events, an incident response strategy must be in place.

**A few preventative measures that can be used for this type of training might include the following:**

1. Use security software to protect your PC. Configure the program to automatically update so that it can cope with any new security concerns.

2. Safeguard your phone by configuring the software to automatically update. These upgrades may provide you with vital security protection.

3. Use multi-factor authentication to secure your accounts. Some accounts provide additional protection by needing two or more credentials to log in. This is referred to as multi-factor authentication. Multi-factor authentication makes it more difficult for scammers to access your accounts if they have your login and password.

4. Back up your data to protect it. Back up your computer's data to an external hard drive or the cloud. Back up your phone's data as well.

**Works Cited:**

<https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams>

<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>