Computer/Phone Phishing and Ransomware Top Employee Security Concerns

First Steps To Computer Security : Lock Your Computer When Stepping Away, And Do Not Leave Passwords On Your Desk

- If you walk away from your desk, even for a brief moment, do you lock your computer? You may not think it's a big deal, but leaving your computer unlocked is a lot like leaving your car running with the doors unlocked. Anyone could sit at your computer and gain access to your private information.
- 81 percent of office employees have access to documents containing sensitive workplace information – and leaving your computer unlocked is a great way to expand who has access to this information.
- Store written passwords out of site of others.
- How do you lock your computer? One of the easiest ways to quickly lock you computer is by holding down the Windows and L key on you keyboard.

What is Phone Phishing?

- Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. It is sometimes referred to as '**vishing**',-a word that is a combination of "voice" and phishing. Voice phishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations known to the telephone company, and associated with a bill-payer. Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.
- Some fraudsters use features facilitated by Voice over IP (VoIP). Features such as caller ID spoofing (to display a number of their choosing on the recipients phone line), and automated systems (IVR Interactive Voice Response).
- Voice phishing is difficult for legal authorities to monitor or trace. To protect themselves, consumers are advised to be highly suspicious when receiving messages directing them to call and provide credit card or bank numbers—vishers can in some circumstances intercept calls that consumers make when trying to confirm such messages.
- It is difficult to ignore a ringing telephone. While fraudulent emails and unwanted mail can be deleted or tossed in the trash, telephone calls are tougher to tune out. And because telephone calls are still considered a secure form of communication, voice phishing scams take advantage of consumers' trust to steal money and personal information.
- In voice phishing—or "vishing"—scams, callers impersonate legitimate companies to steal money and personal and financial information. And these scams are on the rise. In fact, the Federal Trade Commission reports that 77 percent of its fraud complaints involve contact with consumers by telephone.

Phone Phishing Examples

- Typically, when the victim answers the call, an automated recording, often generated with a text to speech synthesizer, is played to alert the consumers that their credit card has had fraudulent activity or that their bank account has had unusual activity. The message instructs the consumers to call a specific phone number immediately. The same phone number is often shown in the spoofed caller ID and given the same name as the financial company they are pretending to represent.
- When the victim calls the number, it is answered by automated instructions to enter his or her credit card number or bank account number on the key pad.
- Once the consumer enters a credit card number or bank account number, the visher has the information necessary to make fraudulent use of the card or to access the account.
- The call is often used to harvest additional details, such as security Personal identification number (PIN), expiration date, date of birth, etc.
- In an attempt to persuade their victims. Posing as an employee of a legitimate body such as the bank, police, telephone or internet provider, the fraudster attempts to obtain personal details and financial information regarding credit card, bank accounts (e.g. the PIN) as well as personal information of the victim. With the received information, the fraudster might be able to access and empty the account or to commit identity fraud. Some fraudsters may also try to persuade the victim to transfer money to another bank account or withdraw cash to be given to them directly.

Phone Phishing Examples (cont.)

- Another simple trick used by the fraudsters is to ask the called parties to hang up and dial their bank, but after the victim hangs up, the fraudster does not, keeping the line open and remaining connected when the victim picks up the phone to dial. When in doubt, calling a company's telephone number listed on billing statements or other official sources is recommended, as opposed to calling numbers received from messages or callers of dubious authenticity. However, sometimes hanging up and redialing is insufficient: if the caller has not hung up, the victim might still be connected, and the fraudster spoofs a dial tone down the phone line to entice the victim to dial. Then the fraudster's accomplice answers and impersonates whomever the victim is trying to call.-This is known as a 'no hang-up' scam. Hence consumers are advised to use a different phone when dialing a company's number to confirm.
- Bank account data is not the only sensitive information being targeted. Fraudsters are also trying to obtain security credentials from consumers who use Microsoft or Apple products by spoofing the caller ID of Microsoft or Apple Inc.

How To Prevent Phone Phishing?

- When a caller claims to represent a specific company, ask for his or her name or employee number and call the company back using an independent and trusted source, like your billing statement or the phone book. Do not call the number provided by the caller.
- Avoid providing personal or financial information over the phone, especially if you did not initiate the call.
- If someone claims you owe a debt, remember that both state and federal laws provide you certain rights when you are contacted by a debt collector, including the right to receive written verification of the debt.
- Remember that in general, you cannot win a prize if you did not enter a contest.
- If you are not sure about the legitimacy of a call, tell the caller you need time to think things over. Ask a co-worker or manager for their perspective.
- Don’t be afraid to hang up if something doesn’t seem right. If it sounds “too good to be true,” it probably is. Never give out your Social Security number or Medicare number to an unsolicited caller. The Center for Medicare and Medicaid Services and the Social Security Administration will not call you to update your information or give you a new card.

What is Phishing?

- The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- There are several types of Phishing.
- Spear Phishing - is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.
- Whaling - is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker.
- Among the types of attacks that workers often fall for, "phishing, spear-phishing and/or whaling" is number one.

Phishing Examples

- Phishing can happen with people clicking on links in emails, but also via social media and even phone calls.
- Scammers like to use social engineering to make their victims jump to attention and get hearts racing. The most common tactic cyber attackers use is creating a sense of urgency, pressuring or rushing people into making a mistake.
- This can be a phone call where the attacker pretends to be the IRS stating your taxes are overdue and demanding you pay them right away, or pretending to be your boss, sending you an urgent email tricking you into making a mistake.
- Research shows that workers tend to lower their guard when money is involved. Attached invoices requesting payment, payment confirmation and document sharing remain difficult for users to avoid.

What is Ransomware?

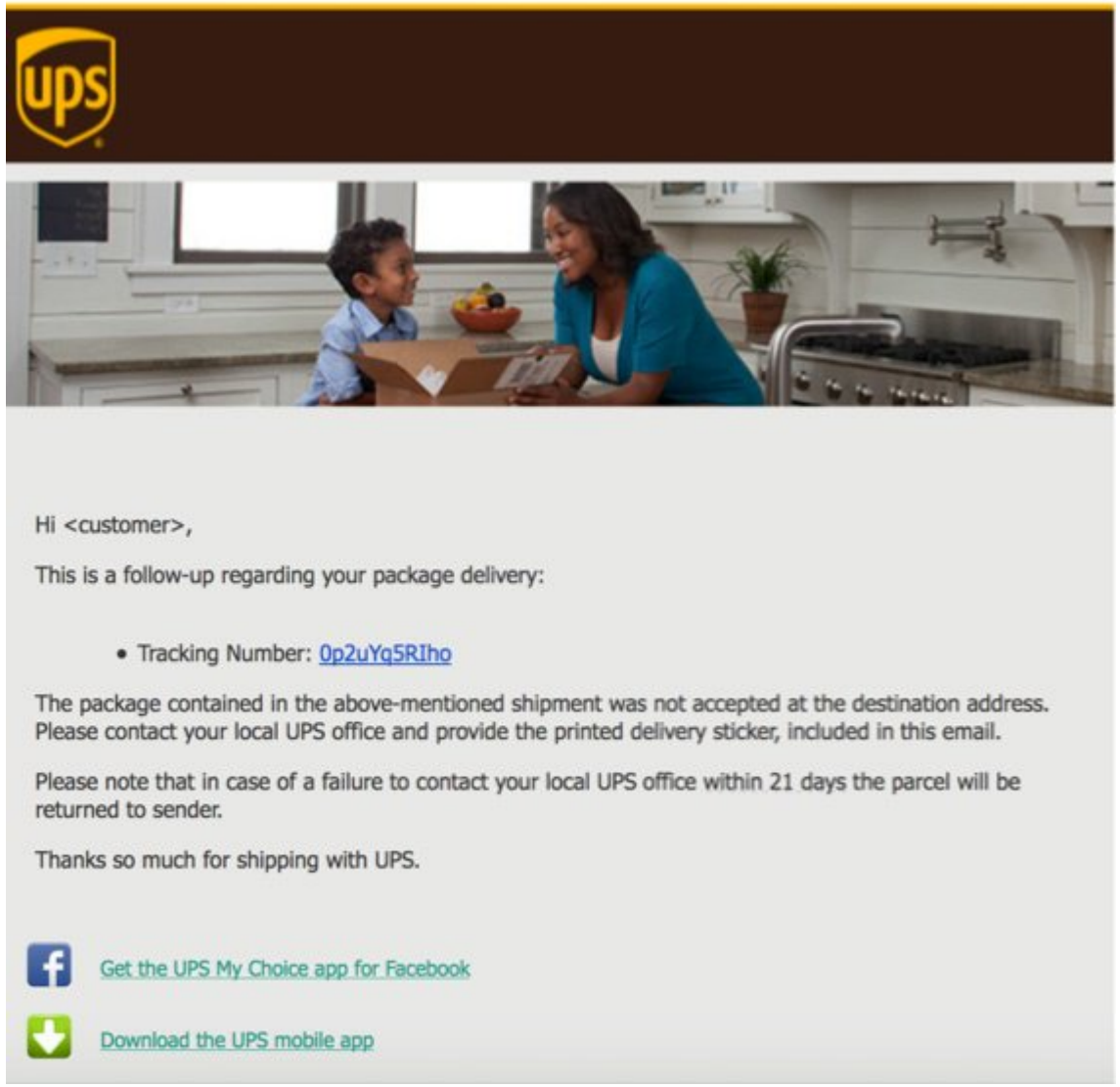
- It is a type of malicious software designed to block access to a computer system until a sum of money is paid.
- There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

Ransomware Examples

- Some attackers don't care much for stealing valuable information. Instead, they use malware that encrypts a victim's files and holds them hostage without ever transferring the data. They demand a ransom for the encryption key that restores access to those files, hence the term ransomware. The user is presented with a message explaining that their files are now are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker. More than a quarter (26 percent) of ransomware attacks hit business users in 2017. Between the second quarter of 2016 and second quarter of 2017, small and midsized businesses paid over $300 million to ransomware attackers.
- WannaCry - WannaCry was one of the biggest cyber security stories of 2017. The WannaCry outbreak began on Friday, May 12, and the ransomware affected hundreds of thousands computers worldwide in a matter of hours.
  The ransomware was particularly virulent because of its ability to spread across an organization’s network by exploiting a critical vulnerability in Windows computers. The vulnerability had been patched by Microsoft in March, but the attackers took advantage of the fact that many systems remained unpatched.

WannaCry


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37



Click on your tracking number and your device is immediately infected with malware

PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

Adding a payment method
Adding a billing address

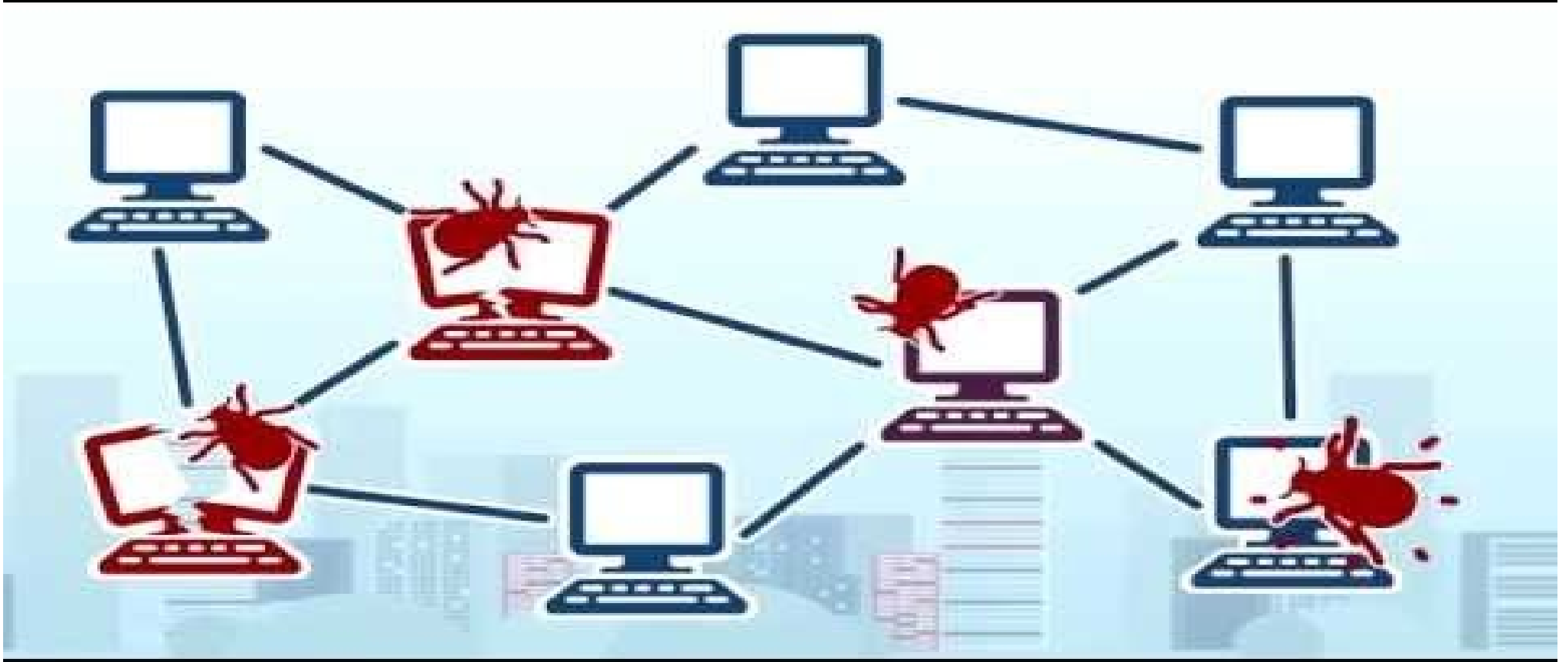
Sending payment
Accepting payment

What can we do?

- Maintaining regular backups, makes ransomware more of an inconvenience than a cripplingly expensive cybersecurity incident.
- Weak, reused and easily guessed passwords continue to be a major security weak spot. A 2017 study found that 30 percent of CEOs had a service linked to their company email hacked and the password leaked. Another survey found that nearly half (46 percent) of employees use personal passwords to protect company data.
- When a caller claims to represent a specific company, ask for his or her name or employee number and call the company back using an independent and trusted source, like your billing statement or the phone book. Do not call the number provided by the caller.
- If you are not sure about the legitimacy of a call, tell the caller you need time to think things over and check with others. Don’t be afraid to hang up if something doesn’t seem right, and they refuse to give you time to think it over.
- If someone claims you owe a debt, remember that both state and federal laws provide you certain rights when you are contacted by a debt collector, including the right to receive written verification of the debt.
- Never give out your Social Security number or Medicare number to an unsolicited caller. The Center for Medicare and Medicaid Services and the Social Security Administration will not call you to update your information or give you a new card.

What can we do?

- **Think Before You Click!** – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead? A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with "Dear Customer" so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.
- **Never Give Out Personal Information** – As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. When in doubt, go visit the main website of the company in question, get their number and give them a call. Most of the phishing emails will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with "https".



Questions?