ISSUE 58 NOVEMBER 2022

RJ2 TECHNOLOGIES

Newsletter

What's Inside:

This month's perspective is brought to you by:
RJ2 Technologies President, Jeff Dann

How to Identify Dangerous Phishing Emails

Phishing is a common scam that involves attempting to trick you into giving away personal, financial, or other sensitive information. It's done by sending an email or posting a link online to make it look like it's coming from someone you know or trust, like your bank, an online payment site or even friends and family members. Phishing emails can look legitimate, but there are some telltale signs to look for.

What is Phishing

Phishing is a scam where criminals send emails that look like they are from legitimate companies, banks and other institutions, but actually contain links to malicious websites. Phishing emails contain links or attachments that lead to malicious websites or install malicious software. Many phishing emails are designed to trick you into providing your personal information (like usernames and passwords) to gain access to your personal data.

To protect yourself from being tricked by phishing scams, you should never click on any links within an email unless you're certain it's safe.

Phishing emails can look legitimate, and there are some telltale signs to look for:

- Check the email address it's sent from
- Look for suspicious links or attachments
- Look out for poor grammar
- The email asks for personal information
- Demands urgent deadlines or threats

Look at the email address it's sent from.

The first thing you want to do is look at the domain name. If it's from a legitimate company, it will be from their official email address. For example, if you were shopping for shoes at Zappos and received an email about your order status in your inbox, that would be sent from "@zappos.com" or "@zappos-support.com."

If you receive an email that looks like it came from these domains but with some sort of grammatical error (for example "your@emailaddress@zappos-support"), then this could actually be an indicator that something fishy is going on with the message and it should not be trusted! Many times, these messages will have small grammatical errors that mirror those of a legitimate company, but they have switched two letters around or misspelled one letter/word (for example "Micorsoft" instead of "Microsoft").

If looking at the domain name does not seem right to you, then check out other clues such as where the message was sent from (the sender's address), who sent it out (the From field) and if there was any attachment included with the message itself - all three-offer valuable insight into whether or not this is truly coming from your bank or airline (or whoever else).

Suspicious links or attachments

Phishers often try to make their emails look like official communications from banks, insurance companies, or other institutions.

Continued on page 2.

CONTINUED...

They may also use names of well-known companies or organizations as part of their scheme. The goal is to entice victims into taking action, and they're very good at it! You should be wary of any email that asks you to click on a link or open an attachment; these are common ways phishers trick you into downloading malware onto your computer.
If you receive an email with a suspicious link or attachment, don't click on it! Delete the message immediately instead. If you clicked on a link or opened an attachment in the suspicious email, your computer may be infected with malware. If this is the case, we recommend that you scan your system with antivirus software. If you have any questions about phishing emails or suspicious links, please feel free to contact us.

Look for poor grammar

If you receive an email with poor grammar, it may be a phishing email. Phishing emails are often riddled with spelling or grammatical errors and often appear to originate from non-English speaking countries. If you receive an email that looks like it was written in another language, do not open it. Instead, forward the message to your IT department for analysis.

The email asks for personal information

If you receive an email asking for your login credentials or payment information, delete it immediately. Never click on links in emails and always check the URL to make sure it's legitimate before entering any information.

Watch for urgent deadlines or threats

When you receive a message that's urgent, it's natural to want to respond quickly. But remember this is a phishing email and the sender is trying to trick you into clicking on the link or attachment. Phishers use fear, threats, and urgency to get your attention and prompt you into responding quickly.

You may also be asked for personal information such as your credit card numbers or social security number in order to verify that the request is legitimate. These requests are often made under pressure from time constraints (like an alleged problem with your account) or threats (such as having money taken out of your account or suspended).

Reduce the Risk of Falling Victim to Phishing Emails

Phishing is a constant threat and the best way to prevent it is through employee training. Hold regular staff awareness modules and ensure that all employees are aware of the dangers of phishing emails.

For a more comprehensive approach to preventing phishing, partner with an MSP (managed service provider) who has email protection on all your endpoints. This will help you reduce risk and protect against threats like social engineering attacks, which use email as a conduit for distributing malware or enabling remote access.

Conclusion

In conclusion, there are many ways to identify phishing emails. The best way to avoid falling victim to a scam is by educating yourself about how these attacks work and taking the time to look at each email before responding or clicking on links.

RJ2 SPOTLIGHT

Joel Pabst:
Dispatcher

Joel Pabst has been a part of the RJ2 team since 2012. He graduated from Trinity International University - IL, where he studied Pastoral ministry. He started as a Jr. Recruiter for the company before moving to Database Management. Since graduation, Joel has not only continued his responsibilities but has also assisted in Marketing, Documentation, and Accounting.

Fun Fact: Joel enjoys long walks on the beach and attending concerts with friends.

Where's your favorite place in the world?
- My bed

What do you like to do when you aren't working?
- Going to the movies, concerts, gaming

What is the best career lesson you've learned so far?
- Teamwork makes the dreamwork

If you could meet anyone in the world, dead or alive, who would it be and why?
- Paul Thomas Anderson, one of my favorite film directors and would be interesting to meet and get inside his head for how he writes and makes movies.

What is your favorite part of working at RJ2?
- The sense of family and teamwork on display

Why Cybersecurity For Insurance Companies Should Be a Top Priority

We Need To Rethink Cybersecurity

Cybersecurity is more than just preventing data breaches. It's about creating a culture of security, making sure your company is prepared for any kind of attack and taking steps to mitigate risk. As an insurance company, you have a unique perspective on cybersecurity. You're in the business of protecting your clients' information, which means you know how important it is that they feel confident their data is safe with you. This is why it's critical that you take your cybersecurity seriously and make sure your clients know it's a priority for you as well. Here are some tips on how to do just that:

Make cybersecurity part of your everyday culture. In order to protect yourself from cyber attacks, it helps if everyone in the company knows what's going on and knows what to do when something happens. Make sure your employees are educated about security threats by offering training courses or providing periodic updates on current threats through email or newsletters. Be proactive about security measures at all times — not just during emergencies. Make sure all employees understand their roles in protecting the company from cyberattacks by providing regular updates on current threats through email or newsletters, holding meetings or presenting videos highlighting best practices for staying safe online and reminding them to update software regularly.

Potential Data Breaches in the Insurance Sector

The insurance industry is at a higher risk of data breaches than other sectors and a recent study by Accenture revealed that the insurance industry could lose as much as $400 billion in revenue.

Insurance companies have a lot of sensitive data to protect, including personally identifiable information (PII), credit card numbers, bank account information and more. These companies are also heavily regulated by state and federal agencies, which means they have strict privacy policies in place and must comply with many different laws regarding the protection of customer data. If you work for an insurance company, you need to be aware of the potential risks your company faces in terms of cybersecurity. Here are some of the most common types of cyberattacks on insurance companies:

Phishing attacks – The most common form of phishing attack involves an email that looks as if it's coming from within the company but is actually from someone trying to gather sensitive information such as usernames, passwords or other PII from employees. This type of attack could result in theft or loss of data or money and can lead to identity theft or fraud against customers or employees.

Malware – Malware includes viruses, worms, trojans, rootkits or spyware that can infiltrate a computer system through various means including email attachments or links to malicious websites. Malware often has the ability to access sensitive information stored on your computer without your knowledge.

Data breaches are a growing concern for businesses, but they can be especially damaging to insurance companies. If a breach results in the loss of customer records, it could potentially harm the company's reputation and result in a significant drop in sales. As such, cyber security is critical for insurance companies to protect their data and ensure that their customers remain confident in their services. The industry has a significant amount of data and sensitive information on its hands, which makes it an attractive target for hackers and cyber criminals. Insurance companies have always been among the most attractive targets for cybercriminals because they have access to confidential data about their clients, such as their personal information (names, addresses and Social Security numbers) and financial records (bank accounts). This can be used maliciously by criminals who want to commit fraud or steal money from unsuspecting customers.

Consumer Confidence Can an Affect an Insurer's Financial Performance

Cybersecurity is a critical component of any business, but it's especially important for insurance companies. Cybersecurity is an integral part of an insurer's operations. It's how they protect their customers' data and their own systems. If a cyber-attack impacts an insurer's ability to fulfill its obligations to their customers, it can have a significant, negative impact on the company's financial performance. Insurers also face reputational harm when they fall victim to a cyber-attack or fail to prevent one from happening. This can lead customers to question an insurer's ability to protect them against cybercrime, which may cause them to shop around for coverage elsewhere.

A recent study by Marsh found that 80% of consumers said they would consider switching insurance companies if they had personal information stolen from one carrier and not another. In addition, consumer confidence can affect an insurer's financial performance through higher claims costs associated with fraud and identity theft or lower premiums because consumers feel more secure about their personal information being protected by the company that insures them.

Why Are Cyber Threats Different For Insurance Companies?

Insurance companies have unique risks associated with cyberattacks because they handle sensitive personal data — including medical information — that can be used by thieves to commit identity theft or fraud. The Equifax breach revealed the vulnerability of our personal data when it's collected by credit agencies like Equifax, Experian and TransUnion. Credit reports are used by lenders when deciding whether to grant loans or mortgages, so it's critical that this information stay secure at all times. In addition to identity theft, stolen credit card numbers also put consumers at risk for fraudulent purchases made with their accounts without their knowledge or consent.

Tips to Secure Your Email

Today, email is one of the most commonly used forms of communication. It's quick, easy and convenient, but it is also vulnerable to attacks from hackers. Here are some practical tips that can help you secure your email account and keep your information safe.

Use Strong Passwords

Many email users fail to understand the importance of using strong passwords. A large number of people still use weak passwords, such as "123456," "qwerty," or even just "password." What's worse, they often reuse these same passwords for multiple accounts—this makes all the accounts vulnerable. To keep all password-protected accounts secure, utilize strong passphrases that are unique to each account. Enabling multi-factor authentication (MFA) for your email account is a good security practice. With MFA, you must provide both your username and password as well as a valid fingerprint scan or answer to a security question when logging in. This makes it more challenging for malicious actors to access your account.

Encrypt Emails

Email encryption is a process that transforms readable text into unreadable code. This code can be read only by someone who has the corresponding decryption key, keeping your email safe from unauthorized access. Email encryption is available with most popular email services, including Gmail and Outlook. The method of encryption varies from service to service but all of them follow a similar approach. Here's how it works: Email encryption involves two phases — first, the sender uses an encrypted email address to send their message to the recipient, and second, the recipient receives the message and decrypts it using their own private key.

Cybercriminals know that email is the most frequently used business communication channel. They also know that most people don't think about protecting their email accounts until they experience a cyberattack. If you are one of those people, it's time to change your ways! Your email account is not as secure as you think it is. The truth is that cybercriminals can target your email account and steal sensitive data or install malware on your device, even if you have a strong password and enable two-factor authentication (2FA). The good news is that there are several ways to protect your email account from cybercriminals, including:

Always install the most recent updates for your antivirus, firewalls, and email security software. Doing so can protect you from cyberattacks, as it enables these cybersecurity solutions to detect and filter out even the newest email-based cyberthreats. Installing these updates also fixes software vulnerabilities that can be exploited by hackers.
Enable 2FA authentication for all accounts that support it. This extra layer of security provides an additional way to verify that someone trying to access your account is really you.

Don't Click on Suspicious Links and Email Attachments

Email accounts are one of the most common target for attackers...

There are many ways to secure your email account, but the most important thing to keep in mind is: do not click on suspicious links and email attachments. Here are some tips to help you keep your account safe:

Do not open unfamiliar emails or attachments from people you don't know. You may receive a phishing email from someone claiming to be an organization (e.g., PayPal, eBay) asking for your login details or a password reset link. Delete these emails immediately. If you receive an email from someone claiming to be PayPal, eBay or any other organization asking for your login details or password reset link, do not click on any links or attachments sent with the message and delete it immediately. Do not open any attachments unless you know exactly what they contain and where they came from. Attackers can send malicious files that look like legitimate files but they actually install malware on your computer when clicked on by users – this can allow them access to everything on your device including personal data stored in your email account (such as messages sent and received).

Beware of Phishing Scams

Phishing is an online scam in which criminals pose as legitimate businesses or individuals to obtain personal information, such as passwords or credit card numbers. Phishing scams can use different communication platforms, but they often involve fake emails that contain links to spoofed websites. When unsuspecting users input their personal information into these fake sites, criminals can use that information to commit identity theft or fraud. Phishing scams are becoming increasingly common, so it's important to be aware of how they work. Take note that reputable companies would never ask for such sensitive data via email. If you believe that the email you received might be from a phishing attempt, contact the company directly using the contact details on their official website. Don't use the contact details in the dubious email as these might be fake too.

Regularly Monitor Account Activity

Monitor for any suspicious behavior, which involves checking your logs for things like unusual devices or IP addresses that have accessed your account. Such activity could indicate a security breach. If you think your account was hacked, sign out of all web sessions and immediately change your password.

Use Different Email Accounts

Don't use one email account for everything. Otherwise, if someone gains access to that account, they could also easily steal any stored information or connected online accounts associated with that email. This could lead to hackers using your account for fraud and other illegal activities. That's why you should create separate email accounts, such as a personal account dedicated to communicating with your friends and family, and a professional account for work-related tasks only. You can also create another email account for miscellaneous things, such as online shops, gaming sites, newsletter subscriptions, and the like.

4 Tips to Improve Your Online Security

Introduction

Online security is a topic that's been getting a lot of attention lately. Data breaches are something you never want to happen, but unfortunately, they're becoming more common. While there's no way to completely prevent these types of attacks, there are some things you can do to make yourself less vulnerable. The following tips will help protect your data and keep your digital life safe:

Following These Tips Will Help Protect Your Data

To help protect your data, follow these tips:

- Use a VPN. A virtual private network (VPN) is a secure internet connection that can be used to connect to public networks. It protects your computer from hackers so they cannot access or steal any personal or confidential information on your device.
- Enable multifactor authentication. This provides an extra layer of protection by requiring two or more pieces of identifying information before granting access to a user account. For example, you may need to enter both a password and an access code sent via text message in order to log in or make changes online.
- Utilize complex passwords that are hard to guess and change them regularly so no one else can guess them either! Complex passwords should have capital letters, lowercase letters and numbers for added security measures against identity theft attempts on social media sites like Facebook or Twitter where many people use simple passwords such as "Password123"
- Install antivirus software as a first line of defense against viruses and other types of potential malware.

Use a VPN

VPN stands for virtual private network. A VPN encrypts your data while you're online, which means hackers have a harder time stealing information from you and your bank account. If someone were to try to intercept the information you send through the internet, it would be unreadable because of how it's encrypted.

A VPN can add an extra layer of protection on top of any other security measures you're using (like multi-factor authentication). They also make sure that when you go online in public places like coffee shops or airports, no one else will know what sites you're visiting or what kind of personal information you may be typing into those sites—unless they've installed their own VPN first!

When you connect to a VPN, it acts as an intermediary between your computer and the internet. You send all of your traffic through the VPN's servers, which means that any third parties who are monitoring or attempting to intercept those communications will see only encrypted data.

You can think of a VPN as an encrypted tunnel between two points on the internet. The tunnel goes through your computer and then out into the open web. When you connect to a VPN, all of your communications go through this tunnel so that no third parties can see what you're doing online.

Enable Multifactor Authentication

Multifactor authentication is a security method that uses two or more sources of identification to verify the identity of a user. This can be done by combining something you know (like a password) with something you have (like your phone), or something you are (a biometric).

Multifactor authentication adds another layer of defense to your account, and it's important for anyone who handles sensitive information like passwords, payment information or other personal details. You may already be familiar with the concept if you use it on your smartphone: when logging in to an app on your phone using Touch ID or Face ID, this is multifactor authentication in action. But there are ways to use it online as well—and they're pretty easy!

Utilize Complex Passwords

To ensure security, you should use a password manager. This software is a secure tool that stores all of your passwords for different accounts in one place. It will generate strong passwords for each account and keep track of them, so you don't have to remember them all yourself.

When creating strong passwords, the best thing to do is combine numbers, letters, symbols and more random characters such as % or !. You should also change your password regularly (at least once every 3 months), especially if it's weak or has been compromised in any way (if it has been stolen or leaked). Additionally, don't use the same password for multiple accounts! For example: don't use "123456" as both your Facebook password and Gmail password because someone who knows one could easily guess the other unless they're very different lengths (e.g., 16 vs 8 characters). Finally – avoid using names ("John"), birthdays ("June 1st")—and anything else that would be easy for someone else to figure out about you!

Tech Tips of the Month

1. Install antivirus & firewall protection
2. Adopt multi-authentication protocols
3. Avoid the usage of public Wi-Fi
4. Regularly backup system data
5. Avoid the insertion of foreign USB devices into the company computers
6. Educate employees on cyber security threats
7. Regularly update all software and operating systems
8. Regularly update passwords

Continued on page 6.

CONTINUED...

Install Antivirus Software

Antivirus software is the first line of defense against viruses, spyware and other types of malware that can steal your personal information or damage your computer. A good antivirus program will automatically scan files as they're downloaded to your computer, alerting you if a virus has been detected. You should also make sure it's up to date, as new threats are discovered constantly.

If you have multiple devices (such as desktop computers and laptops), be sure to install antivirus software on them all. Be careful which apps you install on mobile devices too: many contain malware that can spread like wildfire through unsecured Wi-Fi networks at coffee shops or airports—and then onto any device connected to them!

A top tier antivirus program will include firewall protection, which blocks unauthorized access from outside sources; web filtering so that users cannot access inappropriate websites; parental controls so that parents can limit their children's online activities; identity theft protection services such as monitoring credit reports and alerts when someone tries to open an account using your personal information; automatic backups for important documents stored on computers with access via USB thumb drives so nothing gets lost in case something happens unexpectedly with one machine during its lifespan–and much more depending upon which features.

Conclusion

We hope this blog post helped you better understand the importance of online security and how to keep your data safe. The tips we've outlined can help protect you from hackers, potential identity thieves, and other threats that may target your computer or smartphone.

Featured Partner

ID AGENT
A Kaseya COMPANY

ID Agent's Dark Web monitoring platform provides the most validated credential exposure data available. Its sophisticated intelligence allows companies to focus on their business with peace of mind.