ISSUE 33 FALL 2020

CYBERSECURITY AWARENESS MONTH

RJ2 TECHNOLOGIES

Special Edition: Cybersecurity Awareness Month

What's Inside

9 Tips to Protect Yourself

RJ2 Technologies has the tools and expertise to protect your business from malicious emails.

Below are some suggested guidelines to help protect yourself against these threats when suspicious mail arrives within your mailbox:

1. If you receive a phishing e-mail message, do not respond to it. Don't open junk mail at all!

2. Approach links in email messages with caution

3. Approach images in e-mail with caution

4. Approach attachments in email messages with caution

5. Don't trust the sender information in an e-mail message

6. Don't trust offers that seem too good to be true

7. Report suspicious email

8. Don't enter personal or financial information into pop-up windows

9. Don't forward potentially malicious email messages

Does your business have everything it needs in order to protect itself from malicious emails? Give us a call today at 847-303-1194 to learn more about how we can help.

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

10 Tips for Staying Safe Online

Overlooking your company's online well-being can be a crucial mistake that can cost your business both financially and legally. Luckily, the experienced team of cybersecurity experts at RJ2 have your back.

1. Here's our 10 Tips for Staying Safe Online:

2. Keep tabs on your apps. Update your systems and device applications regularly.

3. Beware of unknown links or attachments in emails. When in doubt, alert your IT or Security Team.

4. Change the manufacturer's default passwords on all of your software and network devices. Ensure websites are SSL-secure (https:// vs http://) before making any financial transactions online.

5. Practice good password management. Refresh passwords every 30 days for all accounts. Security teams, enable Multi-Factor Authentication for all users.

6. Continuously update your personal and company-wide privacy settings. Compliance is an ongoing endeavor!

7. Sensitive browsing such as online banking or e-commerce shopping should only be done on a device that belongs to you.

8. Keep up-to-date on industry trends. Patch vulnerabilities in your devices and software as soon as they become available.

9. Back up your data regularly onsite and offsite.

10. Before connecting to Wi-Fi, take the necessary precautions before accessing corporate or other sensitive data.

Does your business have the necessary knowledge and tools in place to stay safe online? Give us a call today at 847-303-1194 to learn more about how we can help.

FEATURED PARTNERS

Our Featured Cybersecurity Partners:

Learn more about our partners by visiting our website www.rj2t.com/partners!

CYBERSECURITY

Watch out for Distributed Spam Distraction

WHAT IS DSD?

DSD is a type of attack wherein cybercriminals inundate email inboxes with as many as 60,000 spam emails. These emails don't contain dangerous links, ads, or attachments, just random excerpts of text taken from books and websites. But because of the sheer volume of these emails, deleting and blocking each one of them can be daunting. And worse, the email and IP addresses used to send them are all different, so victims can't simply block a specific sender.

NEW TACTICS

Over the years, hackers have developed new DSD tactics. Several reports show that instead of nonsensical emails, hackers are using automated software to have their targets sign up for thousands of free accounts and newsletters to distract them with authentic messages. This allows DSD blasts to slip past spam filters that weed out the malicious code and text used in traditional DSD attacks.

HOW TO PROTECT YOURSELF FROM DSD

DSD is a clear sign that your account has been hijacked, so whenever you receive dozens of emails in quick succession, contact your bank to cancel any unfamiliar transactions and change your login credentials as soon as possible. Also, you should update your anti-spam software (or get one if you don't have one) to protect your inbox from future DSD attacks.

Hackers only initiate DSD attacks after they've obtained their target's email address and personal information, so make sure your accounts and identity are well protected online. You should regularly change your passwords and PINs, enable multifactor authentication, set up SMS and/or email alerts for whenever online purchases are made in your name, and be careful about sharing personal information with others.

DSD is just one of many cyberthreats out there. For expert advice on how to ensure your safety and security online, get in touch with our team of IT professionals.

October

"One single vulnerability is all an attacker needs."
- Window Snyder,
Chief Security Officer, Fastly

TIPS OF THE MONTH

How to protect your business:

1. **Use the contact us form or call RJ2 Technologies today!**
2. **We will run an end-to-end cybersecurity assessment for your business**
3. **We will provide you a clear, concise plan of action - detailling vulnerabillities**
4. **You become a part of the RJ2 Network of Clients**
5. **We provide you with around-the-clock cybersecurity protection across all areas of your business**
6. **Peace of mind for you and your employees knowing RJ2 has your back**