JANUARY NEWSLETTER

RWK IT Services

Vol. 3 Ed. 5 | January 2023

7 Smart Cybersecurity Resolutions for the New Year

These seven good cybersecurity practices will help mitigate a company's risk of a cyberattack and strengthen its security culture.

1. Conduct frequent phishing simulation exercises companywide

Phishing is the most likely launch point for most of today's nastiest cyberattacks including ransomware, business email compromise (BEC) and account takeover (ATO). An estimated 90% of cyberattacks start with a phishing email. Make a commitment to conduct regular training to prepare employees for phishing. To make that training even more effective, customize the content in phishing simulations to reflect the actual threats that employees face daily.

2. Implement or improve a security awareness training program

Security awareness training is one of the primary pillars of building a strong defense for a business. It's affordable and effective. Companies that run regular security awareness training are up to 70% less likely to have a security incident. In order to receive all of the benefits of security awareness training, companies need to make sure that they're doing two essential things: training regularly and training everyone. Putting a security awareness training policy in place that outlines the company's training expectations is a good start to making training work.

3. Invest in MFA

Multifactor Authentication (MFA) has become a critical security measure for businesses and organizations of all sizes and for any individual who use smart devices. When MFA is in place, more than one credential is required prior to granting access to systems or data. After the Facebook security breach in 2018, which exposed user information for over 50 million users, other companies started to add this additional layer of security to their networks.

4. Conduct annual penetration tests

Penetration tests, also known as pen tests are a cyber security technique that organizations can use to identify, test and expose vulnerabilities of their security system and network data. Pen testing is a proactive cybersecurity measure that allows organizations to discover their security weaknesses and take corrective action before an actual cyber attack incident occurs.

RWK IT Services offers FREE penetration tests.

Are you curious about the status of your network security? Contact Jessica at jessica.zemaitis@rwksolvesit.com or 815-205-2155 to schedule your complimentary pen test!

(article continued on page 2)

Employee Spotlight

Goitse aka "G"

Joined RWK - 2022

What is your favorite memory from 2022?
Starting work with RWK. Life changing move!

What are you looking forward to in 2023?
Advancing my responsibilities within RWK. I love helping in any way however I would like to be involved in Projects.

Did you make any New Years Resolutions?
Improve in areas where I lack within RWK. Have a more positive and forward-thinking attitude. Get a new apartment.

What three words would you say describe RWK?
Challenging, fast-paced, friendly personalities. A lot of potential growth to one's career.

What is your favorite thing about RWK?
Learning new technologies. My little tech brain keeps growing with new possibilities and ideas as I get exposed to how things are done around here. RWK also pushes me to think quicker on my feet because of the time constraints on tickets.

Team Celebrations

LET'S CELEBRATE!

Kelly
Anniversary
1/8

Beth
Anniversary
1/10

7 Smart cybersecurity resolutions continued

5. Add dark web monitoring that includes privileged credentials
Credential compromise is a serious problem for every business. Employees love to reuse and recycle passwords, including mixing the use of their favorite passwords between their business and personal lives. Dark web monitoring helps businesses find compromised credentials.

6. Improve email security
The most likely path for a cyberattack to take into a business is via email. Putting the strongest possible email security in place is a powerful way to protect a company from email-based cyberattacks like spear phishing or many types of malware. Secure email gateways are no longer up to the test when it comes to today's sophisticated hackers.

7. Make or test an incident response plan
As discussed in our previous newsletter, we cannot stress the importance enough when it comes to an incident response plan. Making and testing an incident response plan is critical to ensuring that a company can efficiently and effectively respond to a cybersecurity incident.

RWK IT Services can assist with helping your organization complete each of these IT resolutions.

We would be happy to conduct a complimentary pen test or discuss how our managed support or security solutions can put your mind at ease and allow you to focus on your business and not your IT.