RAVENii
CYBER SECURITY

RAVENii NEWS
Phishing Threats Are Rising Dramatically

Bad actors are taking advantage of the drastic, almost overnight shift to working from home.

In a recent survey by Check Point and Dimensional Research, it found that 71% of the 411 Security and IT professionals assessed have noticed an increase in security threats and attacks since the beginning of the pandemic.

Phishing threats made the top of the list at 55%. Hackers are firing around 2600 new threats a day at unsuspecting and information starved individuals.

“The bad guys know that most people are craving information surrounding the coronavirus. They also know that a lot of businesses were unprepared to shift their organizations to remote working with little notice,” says Jeff Shipley, RAVENii’s CEO. “Which means we have a lot of remote workers out in the wild and unprotected.”

Solutions like endpoint protection, employee security awareness training and continuous on-wire monitoring can help ward off these attacks. However, there is more to be considered.

Just like there is no lock that cannot be picked, there is also no security tool that can’t be compromised. Security tools, even when implemented with best practices in mind, are still vulnerable to attacks by adversaries using ever-changing attack vectors and methods. So how do we defend ourselves from phishing attacks?

Shipley says, “Our recommendation is to lead with an operational review of your security policies and procedures. Once those are in place, you can then execute with tool assistance.”

It’s easy to get distracted and even captivated by the blinky lights and the slick marketing propaganda. It is common to feel a sense of security when you believe you have the right security tools in place.

“Tools are tools,” says Shipley. “They are only as effective as the policies and procedures that govern their use.”

That’s why having a set of prioritized security actions to aid you in finding actionable ways to stop today’s most dangerous attacks is a must.

“As a company, RAVENii supports and follows the Top 20 CIS Controls. As an MSSP, we help our clients do the same,” says Shipley. “These controls help us answer the ultimate question of what it is that we need to do to stop known attacks.”

The controls cover most cyber-attack vectors. CIS takes leading threat data from forensic experts across all industries and transforms it into actionable controls to achieve a better overall cybersecurity defense.

The bottom line is we all need security tools to help us manage our cybersecurity initiatives. However, those tools will not be as effective at evading attacks if they are not surrounded by well thought out policies and defined procedures.

If you need assistance in getting a set of prioritized security actions in place, let us know. We are here to help.