Barracuda

10 Ways to Stay Safe Against Ransomware and Other Advanced Threats

It is truly alarming how everyone—individuals, small businesses, right up to global corporations—is now a target for ransomware, phishing, and advanced persistent threats. A successful attack can be terribly costly, and not just financially. Brand reputations—and professional reputations—can be damaged beyond repair.

But there is a lot you can do to reduce the risk. Here are our top 10 tips for preventing ransomware, phishing, and APT attacks:

1 Understand the targets

Whether you're a small business with a handful of employees, or a Fortune 500 company, *everyone* is a target for ransomware. No company or bank account is exempt.

2 Secure all internet threat vectors

Modern, advanced attacks exploit multiple attack vectors including user behavior, applications, and systems. The six main attack vectors are email, web applications, remote users, on-site users, the network perimeter, and remote access. A comprehensive security posture should extend across all these vectors. A firewall is not enough.

3 Secure all attack surfaces

The clear business benefits of migrating to virtual and cloud environments means that hybrid networks are increasingly the norm. Effectively securing cloud or SaaS-based applications like Office 365 requires a comprehensive solution designed to centrally manage hybrid networks.

4 Educate your users

User behavior can be your single greatest vulnerability. Good security is a combination of enforcement, monitoring, and user education—especially against threats like phishing, spear phishing, typo-squatting and social engineering.

5 Don't forget your remote workforce

The mobile revolution drives productivity, collaboration, and innovation, but it means much of your workforce is outside the network perimeter—often connecting via personal devices. This creates a huge potential gap in your security if not properly protected.

6 Keep your systems updated

When vulnerabilities in platforms, operating systems, and applications are discovered, vendors issue updates and patches to eliminate them. Always make sure you've installed the latest, on all potential attack surfaces. And never use obsolete software that is no longer supported with security updates.

7 Detect latent threats

Clean house! Your infrastructure likely contains a number of latent threats. Email inboxes are full of malicious attachments and links just waiting to be clicked on. Similarly, all applications—whether locally hosted or cloud-based—must be regularly scanned and patched for vulnerabilities.

8 Prevent new attacks

With today's evolving threat landscape, sophisticated, targeted, zero-day attacks are coming your way. To stop them, you need advanced, dynamic protection with sandbox analysis and access to up-to-the-minute global threat intelligence.

9 Use a good backup solution

A simple, reliable backup system lets you recover from many attacks within minutes or hours, at very low cost. When data is corrupted, encrypted, or stolen by malware, simply restore from backup and get back to business.

10 Keep management simple

As both networks and threat landscapes grow more complex, it's easy to let security management become a major burden on IT staff. And with complex, disjointed management come more oversights that cause security gaps. Minimize both risk and cost with a simple, comprehensive solution that provides "single-pane-of-glass" security administration and visibility across your entire infrastructure.

Some of these tips may be more challenging to implement than others. Training all your users to practice safe computing—and maintaining that training and awareness over time—may be the most difficult, but it may also bring the greatest benefits.

Barracuda offers many solutions, services, and resources to help you reclaim and secure your network. Contact us to learn how.

US 1.1 • Copyright 2016-2017 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • www.barracuda.com