The 5-Minute Companion for the Cyber-Conscious Employee

ARCTIC WOLF

www.arcticwolf.com

Table of Contents

01 Introduction

02 Phishing: Don’t Take the Bait

03 P@$$w0rd Management: Embrace Complexity

04 Public Wi-Fi: Tread with Care

05 BYOD: Beware of Bad Apps

06 SaaS Selectively: Keep Sensitive Data Safe

07 Plan B: Always Have a Backup

08 You’ve Been Hacked: Now What?

Cyber-consciousness Is Not Innate; It Must Be Learned

Recent studies have pointed fingers at employees, often referring to them as the “weakest link” in cybersecurity. We don’t agree with that wording, and here’s why:

It implicates employees as being careless, when more often than not they haven’t received the proper training.

Much as a business shouldn’t expect a first-day worker to know the ins and outs of its proprietary systems, it’s unreasonable to presume they’re knowledgeable in corporate security best practices.

So, whether you’re an IT manager interested in helping employees improve security hygiene or a professional who’s taken it upon yourself to be more cyber-conscious, this eBook will provide some much needed insight.

Without further ado, here is your five-minute guide to cyber-consciousness.

Phishing: Don’t Take the Bait

Ninety-one percent of cyberattacks start as phishing scams intended to trick users into revealing personal information or downloading malware [1]. Most of these lures are cast through fraudulent emails.

Here are six tips to reduce your chances of being hooked and reeled in by hackers:

- Never share personal information (login and passwords, Social Security numbers, payment card information, etc.) over email.
- Do not download attachments from unknown senders.
- Always consider context, even for messages from known senders. Does Mike from accounting usually send attachments with no text in the body at 10:30 p.m.?
- If an executive requests personal information or a money transfer over email, confirm that request in person or via phone.
- When in doubt, forward on to IT.
- Stay up-to-date on the most recent tactics.

Do these, and you’ll evade hackers’ snares nine times out of 10.

SOURCE: [1] “Dark Reading”

P@$$w0rd Management: Embrace Complexity

When it comes to hacking, 81 percent of data breaches are caused by stolen or weak passwords.[2]

Elude the password-sniffers by sticking to these guidelines:

- Never use a default password. Not even for your IP-connected webcam.
- Create passwords that are at least 12 characters in length. Include letters, numbers and symbols (*$%^~_+). This will fend off brute-force attacks.
- If you have a biometric option (i.e. fingerprint), use it.
- Change your passwords (if they're strong) every six months to a year. [3]
- Use a password manager. If you're an IT manager, make that mandatory for employees. (Pro-tip: LastPass is free. [4])
- Add an authenticator for two-factor protection.

In a cloud-based, app-filled world, a password is often the only barrier between you and a data breach. Keep them complicated and keep them close.

SOURCE:

[2] "Infoworld"

[3] "Wired"

[4] "The Verge"

Public Wi-Fi: Tread with Caution

The ability to work from anywhere is a modern marvel. But if you're connecting to public Wi-Fi (whether at an airport or in a cafe), always err on the side of caution.

- **Be cautious about network selection.**
  Hackers will set up free Wi-Fi networks that appear to be associated with an institution. Ask for the network name if you're unsure.
- **Deactivate public sharing for network discovery, file sharing, printing, and public folders:**

  On Windows: Control Panel> Network and Sharing> Change Advanced Sharing Settings> Public.

  On Mac: System Preferences> Sharing (make sure "file sharing" and " Bluetooth" are off).
- **Browse in a "private" or "Incognito" window to avoid saving information.**
- **If you have a VPN, use it. If you don't, then do not handle any sensitive data.**

If you can help it, avoid public Wi-Fi for work. If you can't, do everything listed above.

BYOD: Beware of Bad Apps

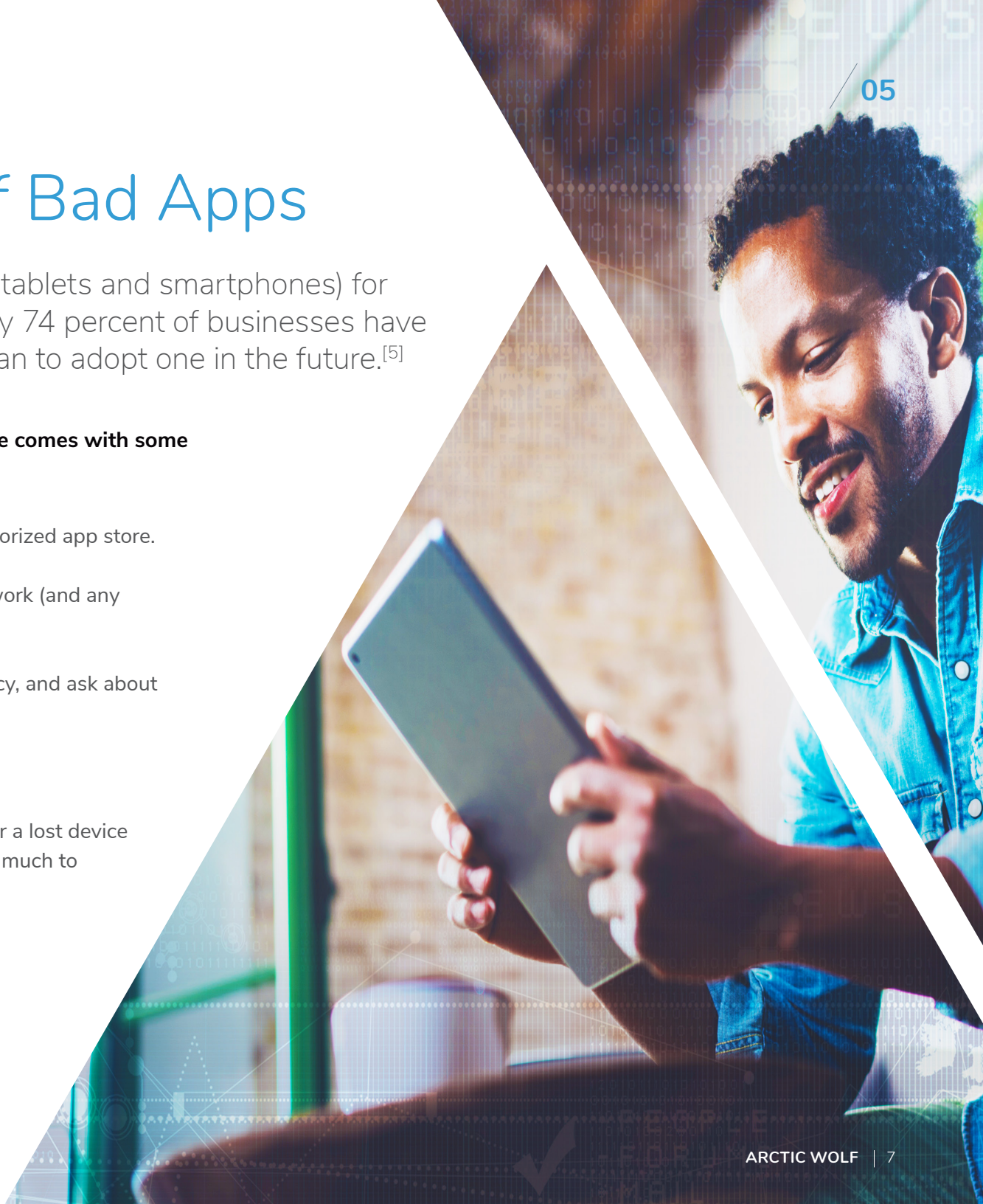
If you use personal devices (laptops, tablets and smartphones) for work, you're not alone. Approximately 74 percent of businesses have bring-your-own-device policies or plan to adopt one in the future.[5]

This opportunity to work on your preferred device comes with some responsibilities. Namely, you must be sure to:

- Only download applications from a trusted, authorized app store.
- Password protect devices that will be used for work (and any device in general).
- Consult your IT department about its BYOD policy, and ask about endpoint protection.
- Do not use untrusted "play" apps.

Whether it's an app from an unauthorized website or a lost device that wasn't password protected, hackers don't need much to compromise critical data.

Give them an inch, and they'll take a mile.



SOURCE:

[5] "ZDnet"

SaaS Selectively: Keep Sensitive Data Secure

Chances are you use at least one cloud-based application (Software-as-a-Service, or SaaS) for work purposes.

Keep those solutions safe, and be mindful of how you access sensitive data.

- Avoid logging into to a SaaS tool on a public computer or public Wi-Fi network.
- Never interact with sensitive data on an unauthorized SaaS application. If you're unsure which cloud-based apps are suitable for use with sensitive data, ask IT.
- Never share your SaaS login credentials with any person over a digital format, or any individual in-person who is not authorized to have them.
- Lock your screen if you step away from your computer during an active session.

Typically, IT is responsible for implementing security controls such as authentication and user access management for SaaS solutions. However, at the end of the day, cybersecurity is a joint effort.

Do your part to keep mission-critical SaaS tools safe.

Plan B: Always Have a Backup

Imagine, to your horror, that an entire day's worth of work is lost in an instant because your laptop has become infected with ransomware at 5:29 p.m.

Unfortunately, horrific scenarios like this are commonplace in 2017, thanks to nasty new strains of ransomware like WannaCry and Petya. Not even a web filter can snag a threat no one has seen before.

To avoid a fiasco, always save your important data to a backup drive. This could be an external hard drive, or more simply, a Dropbox or Google Drive account synced up to your desktop.

Your employer most likely has a backup protocol in place for mission-critical work data. But for your own sanity, back up your BYOD devices, too.

You've Been Hacked: Now What?

If, despite everything, you get hacked (or suspect you've been hacked), take a deep breath, thank your past self for backing up your data, and then jump into action:

- If possible, isolate the device from the network (think airplane mode), shut it down and contact IT right away.
- If that's impossible, (i.e. in a ransomware lockdown) just contact IT.
- Take any additional steps determined by your incident response plan.
- If you don't know your role in that IR plan, ask someone from IT right away.

Every attack requires a different course of action, but it's imperative for an organization to enact a chain-of-command response plan. Non-IT employees need to know how to respond, and that information must come from the top down.

Don't let another day pass without understanding your role in an IR plan. Because even if you can't always keep hackers at bay, you can keep them from beating you.

Industry's Most Fierce SOC-as-a-Service

Security Operation Center (SOC) is the most essential element of modern security. But SOCs are expensive, complicated and far beyond the reach of most small to medium enterprises. So many take the easy route and invest in security products, but not in people and processes required to manage a SOC.

AWN CyberSOC™ differs from traditional managed security services. It is a dynamic combination of world-class Concierge Security Engineers (CSE), advanced machine learning, and comprehensive, up to the minute threat intelligence. Your CSE conducts both routine and non-routine tasks to protect you from known and emerging threats.

AWN CyberSOC™ provides:

- Dedicated Security Expert
- Managed Detection and Response
- Security Incident and Crisis Support
- Regulatory Compliance
- Simple, Predictable Pricing

AUTHORIZED PARTNER

EPC USA

Colorado Sales Partner

+1 303 703 3609

ARCTIC WOLF

www.arcticwolf.com

©2017 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.