Presented by: Nobukhosi Dlamini

www.bahatitech.co.za

Protecting your business from online attacks

A practical approach to protect your business online

BAHATI
TECH

What will we achieve in this webinar

- What are some common risks that my business faces online
- What can I do to protect my business online
- What if I need additional support

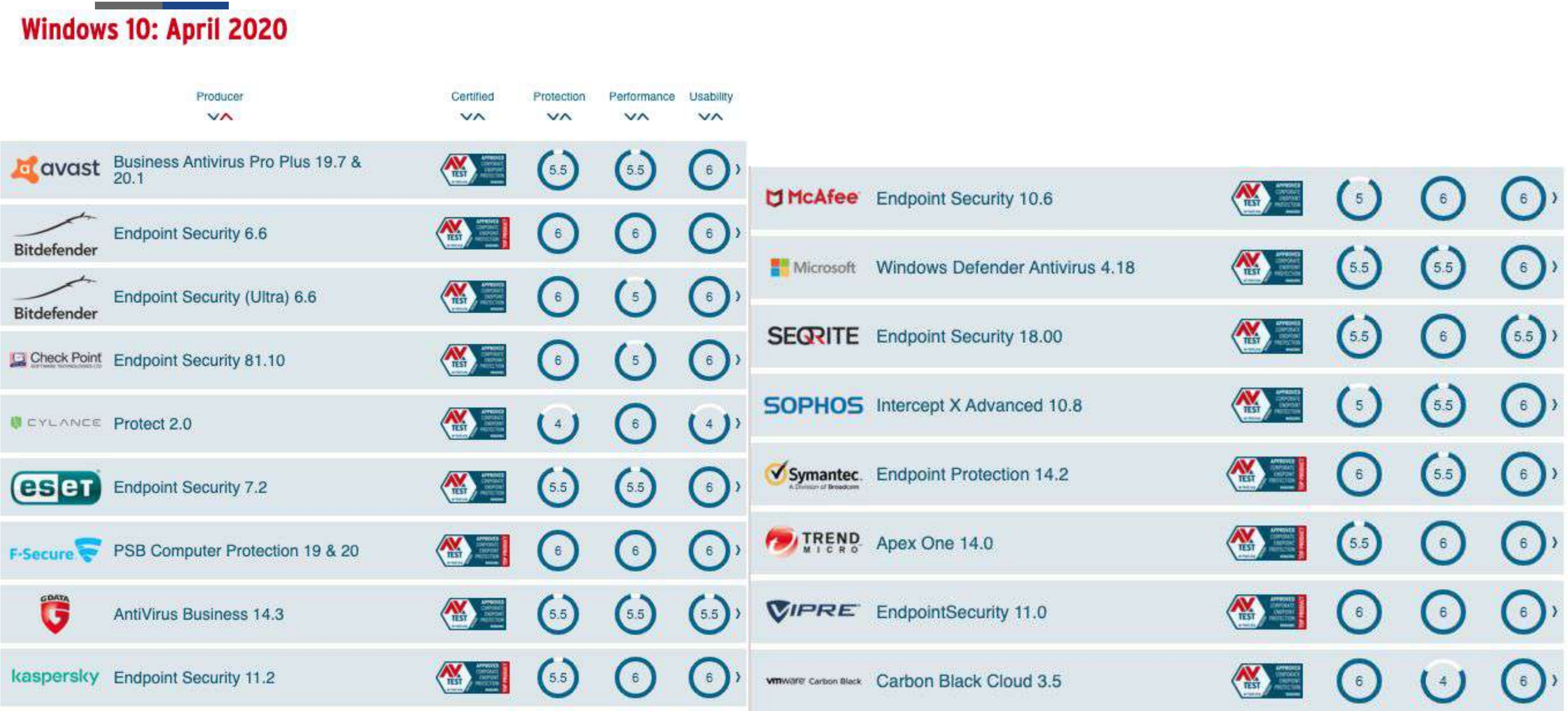
Agenda

1. Three basic principles
2. Common online risks
   a. Lack of knowledge/awareness
   b. Poor password hygiene
   c. Phishing Attacks (Deception)
3. Book one complimentary online security consultation with us (Limited Spots Available)

Three Basic Principles

Keep your "antivirus" updated

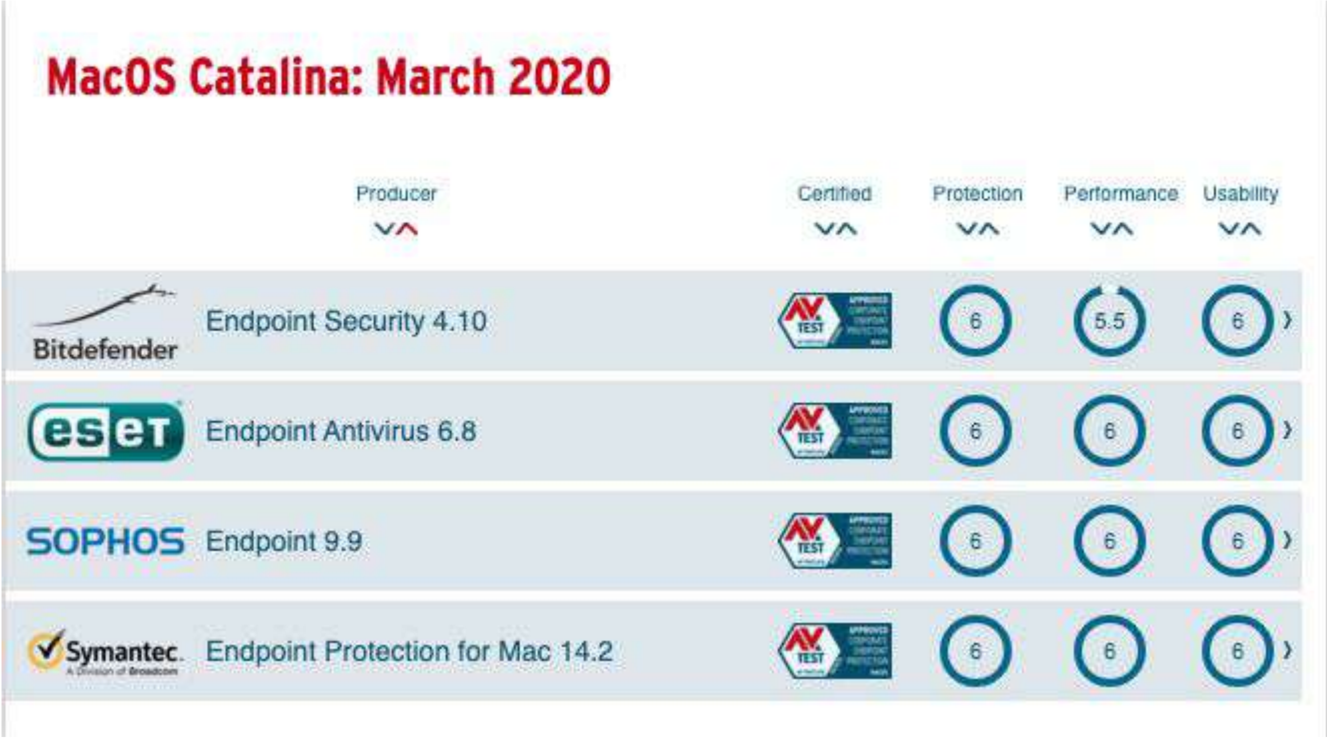
Antivirus performance - April 2020 (Windows Business)



Windows 10: April 2020

Producer		Certified	Protection	Performance	Usability
avast	Business Antivirus Pro Plus 19.7 & 20.1	AV TEST APPROVED	5.5	5.5	6
Bitdefender	Endpoint Security 6.6	AV TEST APPROVED TOP PRODUCT	6	6	6
Bitdefender	Endpoint Security (Ultra) 6.6	AV TEST APPROVED	6	5	6
Check Point	Endpoint Security 81.10	AV TEST APPROVED	6	5	6
CYLANCE	Protect 2.0	AV TEST APPROVED	4	6	4
eset	Endpoint Security 7.2	AV TEST APPROVED	5.5	5.5	6
F-Secure	PSB Computer Protection 19 & 20	AV TEST APPROVED TOP PRODUCT	6	6	6
G DATA	AntiVirus Business 14.3	AV TEST APPROVED	5.5	5.5	5.5
kaspersky	Endpoint Security 11.2	AV TEST APPROVED TOP PRODUCT	5.5	6	6
McAfee	Endpoint Security 10.6	AV TEST APPROVED	5	6	6
Microsoft	Windows Defender Antivirus 4.18	AV TEST APPROVED	5.5	5.5	6
SEQRITE	Endpoint Security 18.00	AV TEST APPROVED	5.5	6	5.5
SOPHOS	Intercept X Advanced 10.8	AV TEST APPROVED	5	5.5	6
Symantec. A Division of Broadcom	Endpoint Protection 14.2	AV TEST APPROVED TOP PRODUCT	6	5.5	6
TREND MICRO	Apex One 14.0	AV TEST APPROVED TOP PRODUCT	5.5	6	6
VIPRE	EndpointSecurity 11.0	AV TEST APPROVED TOP PRODUCT	6	6	6
vmware Carbon Black	Carbon Black Cloud 3.5	AV TEST APPROVED	6	4	6

Antivirus performance - April 2020 (MacOS Business)



MacOS Catalina: March 2020

Producer		Certified	Protection	Performance	Usability
Bitdefender	Endpoint Security 4.10	AV TEST	6	5.5	6
eset	Endpoint Antivirus 6.8	AV TEST	6	6	6
SOPHOS	Endpoint 9.9	AV TEST	6	6	6
Symantec A Division of Broadcom	Endpoint Protection for Mac 14.2	AV TEST	6	6	6

Don't plug in other people's USB drives into your computer

Avoid using public wifi

Lack of awareness

The most dangerous threat for your business is the lack of awareness. Businesses, no matter how small, require some cybersecurity awareness for all staff members. Each employee must be trained for responsible use of the internet. They should be able to identify threats hidden in emails and any software they install on their devices. They should be able to create better passwords and must follow policies pertaining to information sharing.

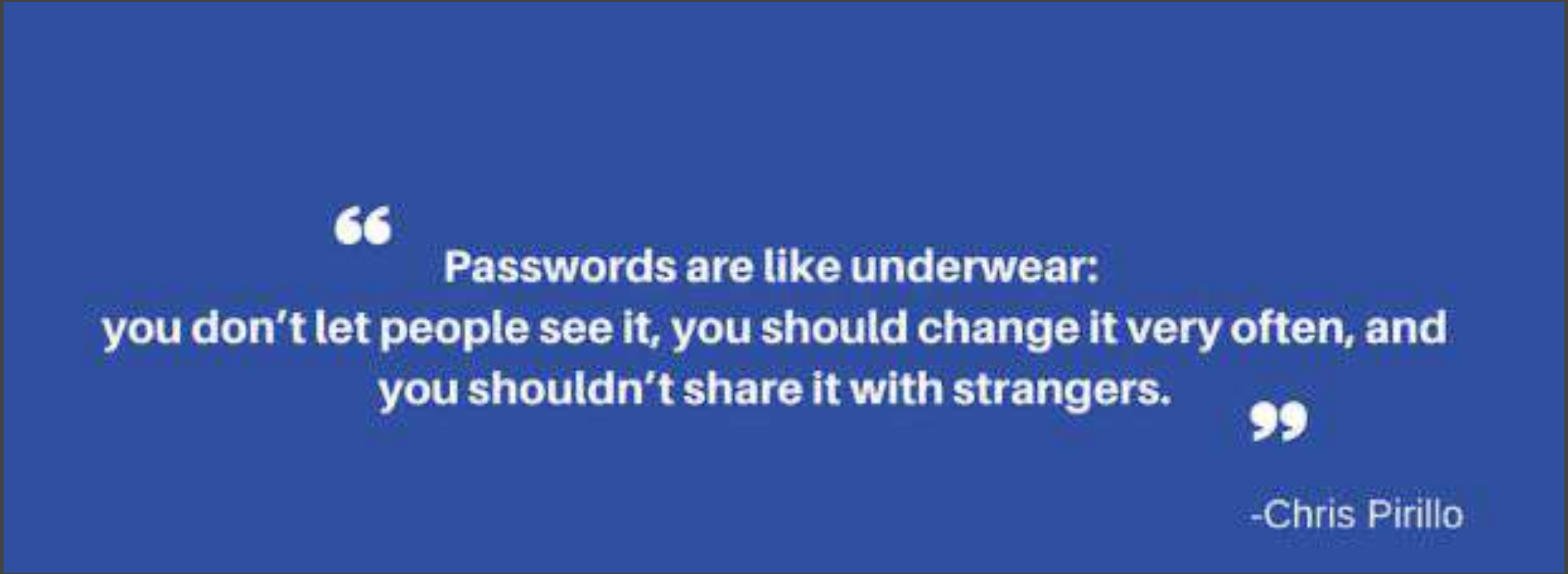
Lack of awareness

1. Lack of policies/ strategy

2. Lack of staff training

3. Lack of skilled personnel

4. Poor technical and organisational controls



> “Passwords are like underwear:
> you don’t let people see it, you should change it very often, and
> you shouldn’t share it with strangers.”

-Chris Pirillo

Common Password Mistakes

1. Using the same password on multiple websites/ apps
2. Letting other people know your passwords/ sharing passwords with other people
3. Non-complex password
4. Personal information e.g. names of relatives, celebrities, sports teams, pet or any other common terms that can be found in the dictionary
5. Recognizable keystroke patterns e.g. “qw3rty”
6. Too short - less than 12-characters
7. Substituting letters for numbers or special characters e.g. “$afe1y”
8. Changing a password with a single character or number e.g. changing an 8 to a 9 or changing a "!" to a "&" at the end of an existing password. Non-alphanumeric characters should be used in the middle of the word not at the end
9. Saving passwords in spreadsheet or emailing it to yourself
10. Not using two-way authentication
11. Not updating passwords regularly

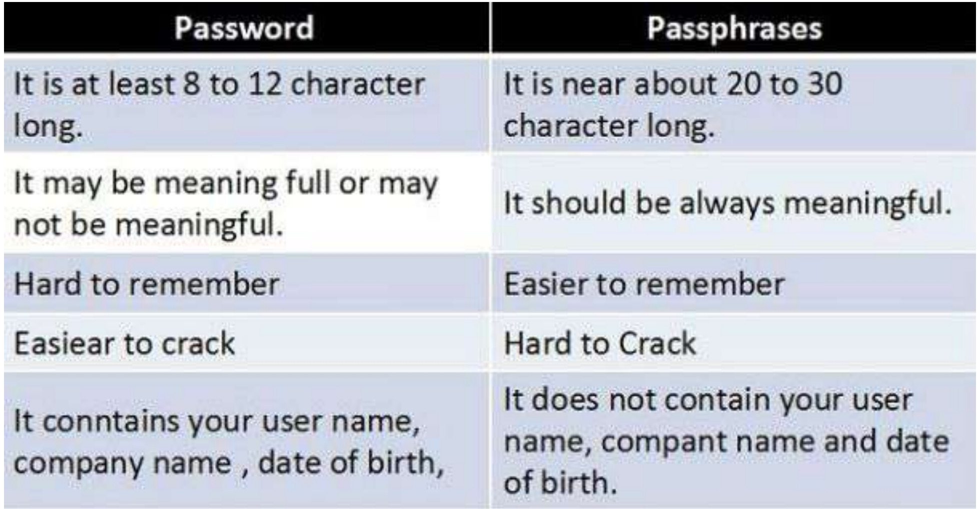
Password vs Passphrase

Humans are generally bad at password management.
Passwords are hard to remember and easy for hackers to crack

Instead of using words use a long paraphrase

A quote or a line song that you like and can easily remember

- Or random passphrase generator e.g. https://www.useapassphrase.com/
- Firefox, Chrome, Safari and Internet Explorer all have built in password managers.. Or find one in the app store
- Use a different passphrase for each site or customize your passphrase for each site



Password	Passphrases
It is at least 8 to 12 character long.	It is near about 20 to 30 character long.
It may be meaning full or may not be meaningful.	It should be always meaningful.
Hard to remember	Easier to remember
Easiear to crack	Hard to Crack
It conntains your user name, company name , date of birth,	It does not contain your user name, compant name and date of birth.

Example

Core passphrase: "gibberish gawk gossip ocean"

Approximate Crack Time: *8,617,333 centuries*

Facebook:	"gibberish gawk FB gossip ocean"
Twitter:	"gibberish gawk TW gossip ocean"
Instagram:	"gibberish gawk IG gossip ocean"
Mailchimp:	"gibberish gawk MC gossip ocean"

Millions of email addresses have been compromised in recent data breaches

E.g. Adobe (153 mil), Canva (139 mil), eBay (145 mil), LinkedIn (165 mil), MyFitnessPal (150 mil), Facebook (540 mil), United Nations (Unknown), Microsoft (250 mil)

Check if you have an account that has been compromised in a data breach, visit

https://haveibeenpwned.com/

If your email address shows up - change all your passwords for accounts where you use this email address

Phishing Attacks

What is phishing?

Phishing is a deceptive scam in which criminals try to get your personal information, such as passwords and financial information.

Phishing attacks usually come in the form of an email or link on social media pretending to be from an official site, such as your bank, but instead lead to a fake website that looks very much like the real one.

How can I protect myself from phishing attacks

1. *Train your staff members so they are aware of the phishing risk*
2. *Legitimate institutions e.g. your bank, will never request your personal information via email. Any unsolicited email, phone call, or mail that does is probably a phishing scam.*
3. *Visit a website by typing it in the URL instead of clicking a link in an email. Although the link may look legitimate, phishers use all sorts of tricks to hide where it's really going.*
4. *Check your credit card and bank statements regularly for fraud.*
5. *Check to make sure your bank account has insurance against fraud*
6. *Report a phishing scam to the real organization. Most banks, social media sites, and other institutions usually have an email address online to report scams, spam, or any other unethical behavior.*

Hundreds of suppliers caught in tender scams

What is a Tender/ RFQ Scam?

Fraudsters use what appears to be government department letterheads with fictitious logos and contact details to send a fake RFQ to a company to invite it to urgently supply goods

How can I protect myself from tender scams

1. *Always double check that the tender/rfq is valid before acting upon it. Don't use the contact details on the tender document as these might be fraudulent. The contact details for all departments are on every government department website*
2. *If you're uncomfortable about the request received, consider visiting the government department and/or the place of delivery and/or the service provider from whom you'll be sourcing the goods.*
3. *Fake tenders use the same or very similar telephone numbers as the government department. Although such number with an area code 012 looks like a landline, it is not fixed to any property*
4. *Check the domain name on the email displayed on the tender vs. the domain name of the department. E.g. a fake tender may display this email address tenders@health.org.za whereas the genuine department domain is www.health.gov.za*
5. *Never pay a deposit to bid for work.*

Contact Details

Book a Free Session:

https://calendly.com/bahatitech/godigitalfollowup

Email: nobukhosi@bahatitech.co.za

LinkedIn: https://www.linkedin.com/in/nobukhosi-dlamini/

Twitter: @bahati_tech

Instagram: @bahatitech @nobukhosi07