Staying Ahead of the Baddies

Bart Busschots

👋 Who am I?

<b> bartificer creations

Day Job

- Maynooth University
  - **Cyber Security Specialist**
  - Linux & Windows Sysadmin (2005 – 2022)
  - Junior Lecturer & Researcher (Computer Science: 2001 — 2005)

Side Hustles

- Bartificer Creations
  - Open Source Software Development
  - IT Consulting
- Let's Talk Podcasts
  - Let's Talk Apple
  - Let's Talk Photography
- Podfeet Podcasts
  - Security Bits segment on NosillaCast
  - Taming the Terminal Series
  - Programming by Stealth Series

20" G4

28" Intel

3G

15 Pro Max

1st Gen

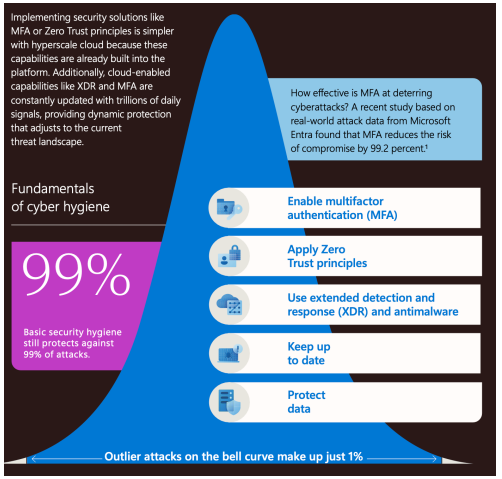
12.9" Pro

S0

Ultra 2

DON’T PANIC — You’re not Powerless

“… the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices” — **Microsoft Digital Defense Report 2023**



Perfect Security is impossible …

but it’s **the basics** that **matter most**!

🤨 Who's Out to get Us?

For the vast majority of us, there's just one threat:

Cybercriminals

The Unlucky Few

- **Business Leaders** — also beware nation states & insider threats
- **Campaigners** — also beware nation states & activists
- **Internet Celebrities** — also beware thrill seekers (website/social media defacement *'for the LOLs'*)
- **Stalking/Abuse victims** — also beware insider threats (the stalkers/abusers)

🤑 What do They Want?

Profit!

- **Money** — by theft or extortion
- **Crypto** — coins or NFTs
- **Data** — for sale
- **Accounts** — for sale
- **Resources** — CPU/RAM/network to power their criminal enterprises

 It's All About Economics

- When your adversary is motivated by ideology, they will relentlessly spend money to attack you
- But when your attacker is motivated by money, they won't spend more than you're worth

We don't need perfect protection, we just need to be economically unappealing!

How Do They Attack Us?

- The squishy organic bit:
  - Trick Us
  - Extort Us

- Our tech:
  - Become Us (take over our accounts)
  - Hack Our Stuff (take over our devices)

 How Can We Defend Ourselves?

1. **Vigilance** — always be alert, be suspicious of the unexpected, and remain rational
2. **Good Digital Hygiene** — the simple stuff really matters!
3. **Digital Literacy** — some basic knowledge goes a long way!

Be Deliberate — make proactive and informed decisions, don't just enable/install things unthinkingly

👀 Defense 1 — Vigilance

- **Follow the money** — if you can’t figure out the finances, stop!
  - Either you're missing something
  - Or it's a scam
- If it seems too good to be true, it almost certainly is!
- Our emotions are their trump cards — watch out for manipulation
  - Anger, Fear, Greed
  - Compassion, Love
- **Don't allow yourself to be rushed**
  - False sense of urgency — *"act now or else …"*
  - Artificial scarcity — *"only 4 left, hurry!"*

🚩 Red Flags

Vigilance

- Anomalous Language
  - Is the tone appropriate to the message?
  - Is the grammar correct?
- Anomalous Knowledge
  - Do they know things they shouldn't?
  - Do they not know things they should?
- Do they usually contact me in this way?
- Does this contact contradict their stated policies/promises?
  - *"we will never ask you for personal info over the phone"*
  - *"we will never ask for passwords over email or SMS"*

Generative AI (ChatGPT …)

Broken English Prompts

↓

Perfect Business Emails

- Poor grammar is still a red flag
- **Good grammar is now meaningless**

😷 Defense 2 — Good Digital Hygiene

1. Passwords
2. Accounts
3. Your Data
4. Software

🔑 Passwords Suck

Digital Hygiene

Passkeys are the future …

but they're not quite ready yet 😕

- Expect fewer passwords over time (but never zero)
- Humans can't manage passwords → **Use a Password Manager!**
  - **Passwords can't be safely re-used** → too many to remember
  - We're too predictable → **use generated passwords**
- **Length is what** matters — passwords need to be long (20 characters), then no need for weird symbols

Passwords are not enough (leaks everywhere) …

2-factor/Multi-factor Authentication is VITAL

Password Managers

- iCloud Keychain is all most people need
  - Mac, iOS & Windows browsers (Edge & Chrome)
- 1Password for Families 👍
  - Easy sharing
  - Mac, iOS, Windows & Android
  - `www.1password.com`

Password Generators

- Built-in KeyChain & 1Password generators are fine
- I like human-readable but strong so I created `www.xkpsswd.net`

2/Multi Factor Authentication (2FA/MFA)

Digital Hygiene

- **2-Factor Authentication (2FA)** — password plus extra factor (becoming Legacy)
  - **Something you have**, e.g. token, device, email address, phone number, certificate …
  - **Something you are**, e.g. TouchID, FaceID …
- **Multi-Factor Authentication (MFA)** — two or more factors, one can be a password
  - Includes all 2FA factors
  - Can also include metadata like your location, device & app
  - Often uses AI to add extra hurdles for *'risky'* logins — *"is this normal for Bart?"* or *"does this look like a known bad thing?"*

The MFA/2FA Hierarchy

- SMS is prone to SIM swapping
- Phishing-resistance is important
- Best → Least-good
  - **Hardware Token** (FIDO)
  - **Passkeys/WebAuthn** (FIDO 2)
  - Push notification with number matching
  - Push notification to app
  - TOTP (**T**ime-based **O**ne-**T**ime **P**assword, e.g. Google Authenticator)
  - Email code
  - Voice call with code
  - **SMS code**

Accounts

Digital Hygiene

- Avoid creating accounts you don't need
- Keep personal & work identities separate
- Delete accounts you stop using
- When possible, use a reputable single sign-on service
  - Sign in with Apple (consider their option to hide your true email address)
  - Sign in with Microsoft/Google work/school account (for work/school stuff)
  - Personal Microsoft/Google accounts (especially if you're a paying customer)
- Don't use social media accounts for single sign-on
  - Avoid sign in with Meta/Facebook
  - Avoid sign in with X/Twitter

👑 The Crown Jewels

- Banking Sites
- Email services
  - Password resets!
- Apple/Google ID
  - Your files & photos!
- Sites you use for sign-in-with

📂 Your Data

Digital Hygiene

- Know what you have, and where it is
- Buy cloud storage from a reputable source
- Use 2FA/MFA on your cloud storage
- Backup, backup, backup — 3, 2, 1 Strategy
  - 3 copies
  - 2 formats
  - 1 in the cloud
- Share with care
  - Don't share more info than you need to!
  - Make share links as specific as possible
    - Avoid ‘anyone’ links
    - Avoid read+write links
    - Prefer time-limited links

👑 The Crown Jewels

- Government ID Numbers (SSN, Passport Number, …)
- Personal Data (DOB, Address, mother’s maiden name, …)
- Financial data (account numbers, …)
- Your iCloud account
- Family Photos

Software (OS)

Digital Hygiene

- **OS updates are vital**
  - Patch early & patch often!
  - **Never use an unsupported OS** — upgrade before security updates stop!
- Use your OS's built-in protections
  - Don't disable full disk encryption
  - Do enable the firewall
  - Don't disable the built-in basic virus protections
- Use a trusted AV on your Mac (not on iPhone or iPad)
  - Protects you from you — you only need to make one mistake once!
  - Stops you spreading bad things to friends and family
  - **AV is like a seat-belt** — it **doesn't make you invulnerable**, but it helps lot!

Software (apps, plugins, extensions etc.)

Digital Hygiene

- Don't Pirate Software — **it's full of malware!**
- Only install software you actually need
- Get your software from reputable sources
  - The official app stores are safest, especially Apple's
  - Trusted major brands are also safe (e.g. Microsoft, Adobe)
  - Long-running trusted open-source projects are safe (e.g. Firefox, VLC)
  - Recommendations from trusted experts are relatively safe
- When outside official app stores, always download directly from the author's website
- **Never install software that you didn't go looking for** — if something pops up out of the blue, say no!
- **Software updates are vital**— patch early & patch often!

Defense 3 — Digital Literacy

- Understand the structure of digital addresses
  - Domain names
  - URLs
  - Email Addresses
- Understand what security indicators actually mean
  - HTTPS — the padlock in the browser
  - Verified Badges (maybe, if we have time)

Domain Names

Digital Literacy

- Order of importance is right to left
- The **apex domain** is what matters — that's what you need to check

Which domains really belong to `mybank.com`?

`www.mybank.com`	✅ `mybank.com` is on the right edge
`ie.support.mybank.com`	✅ `mybank.com` is on the right edge
`my-bank.com`	❌ `mybank.com` isn't in this domain at all
`mybank.com.au`	❌ `mybank.com` isn't on the right edge
`Mybank.com.github.io`	❌ `mybank.com` isn't on the right edge

URLs (Web Addresses)

Digital Literacy

- Always check the Apex Domain — that's the website you're really at
- Simple to find:
  1. Find the first / after the ://
  2. The apex domain is directly to the left

🌐 URLs (Web Addresses)

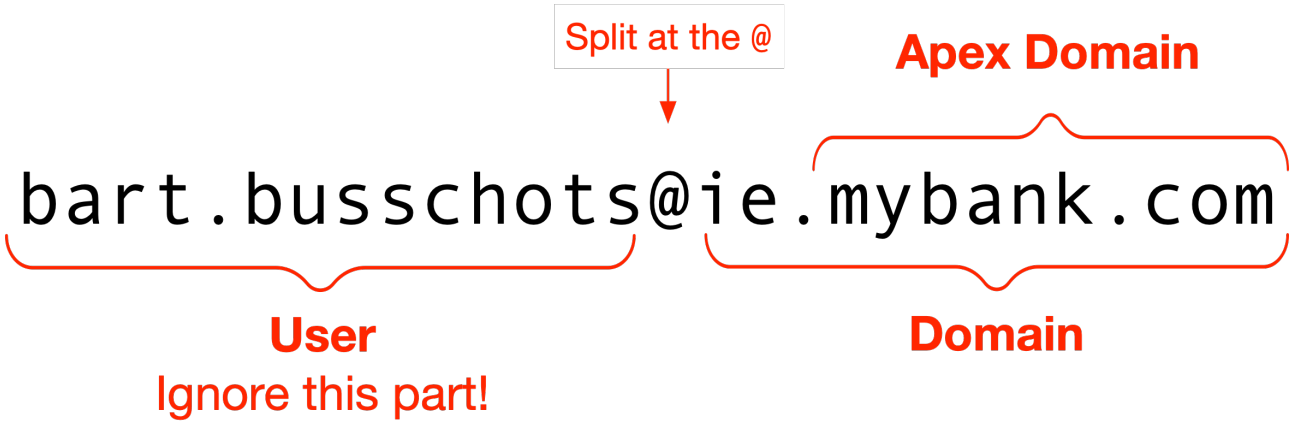
Digital Literacy

Which websites really belong to `mybank.com`?

`https://mybank.com/`	✅ `mybank.com` is directly to the left of the first /
`https://www.mybank.com/login`	✅ `mybank.com` is directly to the left of the first /
`https://www.mybank.com/login?u=2`	✅ `mybank.com` is directly to the left of the first /
`https://mybank-com.co/`	❌ `mybank.com` isn't in the domain at all
`https://mybank.com.bank/login`	❌ `mybank.com` isn't directly to the left of the first /
`https://mybank.com.github.io/test`	❌ `mybank.com` isn't directly to the left of the first /
`https://hosting.com/mybank.com/`	❌ `mybank.com` is to the right of the first /
`https://hosting.com/login?site=mybank.com`	❌ `mybank.com` isn't directly to the left of the first /

Email Addresses

Digital Literacy



- Always check the Apex Domain — that's the email's source
- Simple to find:
  1. Find the @ symbol
  2. Ignore everything to the left of the @, the full domain is on the right
  3. The Apex Domain is at the end of the domain

✉ Email Addresses

Digital Literacy

Which websites really belong to `mybank.com`?

• `tom@mybank.com`	✅ `mybank.com` is the entire domain
• `support@mybank.com`	✅ `mybank.com` is the entire domain
• `tom@support.mybank.com`	✅ `mybank.com` is at the end of the full domain
• `security@mybank.com.co`	❌ `mybank.com` isn't at the end of the domain
• `security@mybank-com.co`	❌ `mybank.com` isn't in the domain at all
• `tom@mybank.com.bank`	❌ `mybank.com` isn't at the end of the domain
• `mybank.com@gmail.com`	❌ `mybank.com` is on the wrong side of the `@`

What Does HTTPS Mean?

Digital Literacy

Three Promises

- **Authenticity** — you really are at the site in the address bar
  - no Machine-in-The-Middle (MiTM)
  - No DNS spoofing
- **Integrity** — the information sent and received can't be changed enroute
- **Confidentiality** — no eavesdroppers

Does Not Mean!

- That anyone has verified the site in any way
- That the site is trustworthy
- That the site's payment systems are certified
- That the site is not criminal
- **That the site is *'safe'***

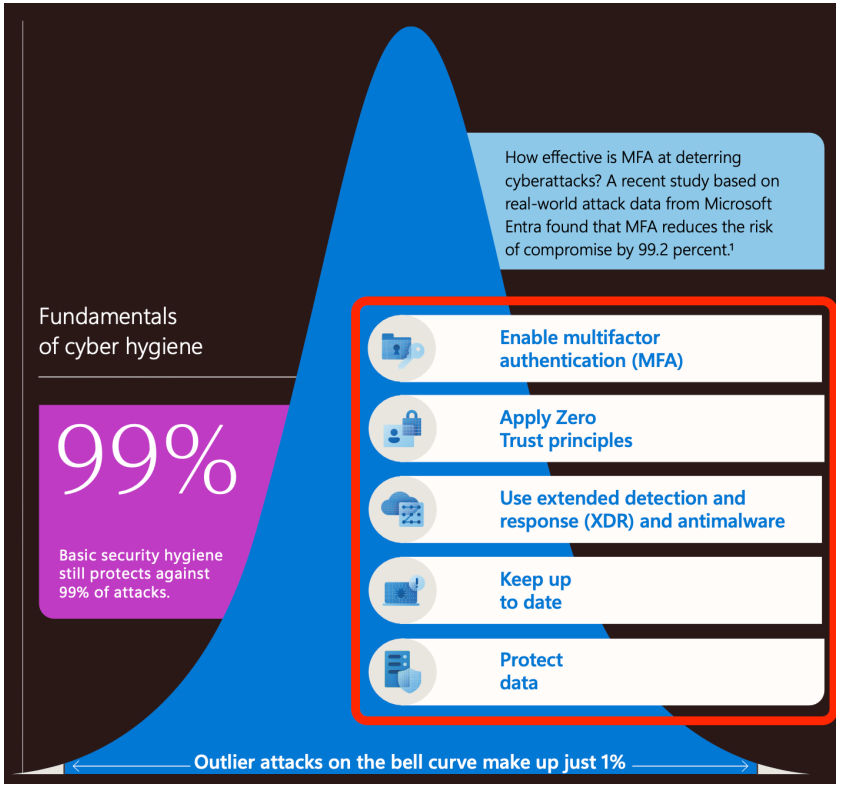
Always check the Apex Domain the address bar!

Password managers won't be fooled by typos or look-alikes

So What are the Basics for Us?

Translating Microsoft's Advice for Home Users

- Use the best 2FA/MFA everywhere you can
- Zero Trust:
  - Password/passcode on all Devices
  - Enable Mac Firewall
  - Separate accounts, don't be Admin day-to-day
  - Separate banking from regular browsing
  - Assume it's a scam
- Install antivirus on your Macs
- Patch early & patch often!
- Protect your data:
  - Enable disk encryption
  - Be sure to use 2FA/MFA on cloud services
  - Know what you have & where it is!
  - Share with care



Questions?

www.bartb.ie

Verified Badges

Digital Literacy

A badge is only as meaningful as the process

- iMessage Verified Sender — *“the message really is from this company”*
- Mastodon Verified Link — *“the profile and the web page are controlled by the same person”*
- Facebook/Instagram Verified Profile/Page — *“the owner has proven their identity to Meta with photo ID”*
- Twitter Blue Tick — *“the owner pays a monthly subscription”* (utterly meaningless!)

⚠ A badge in the wrong place is fake!