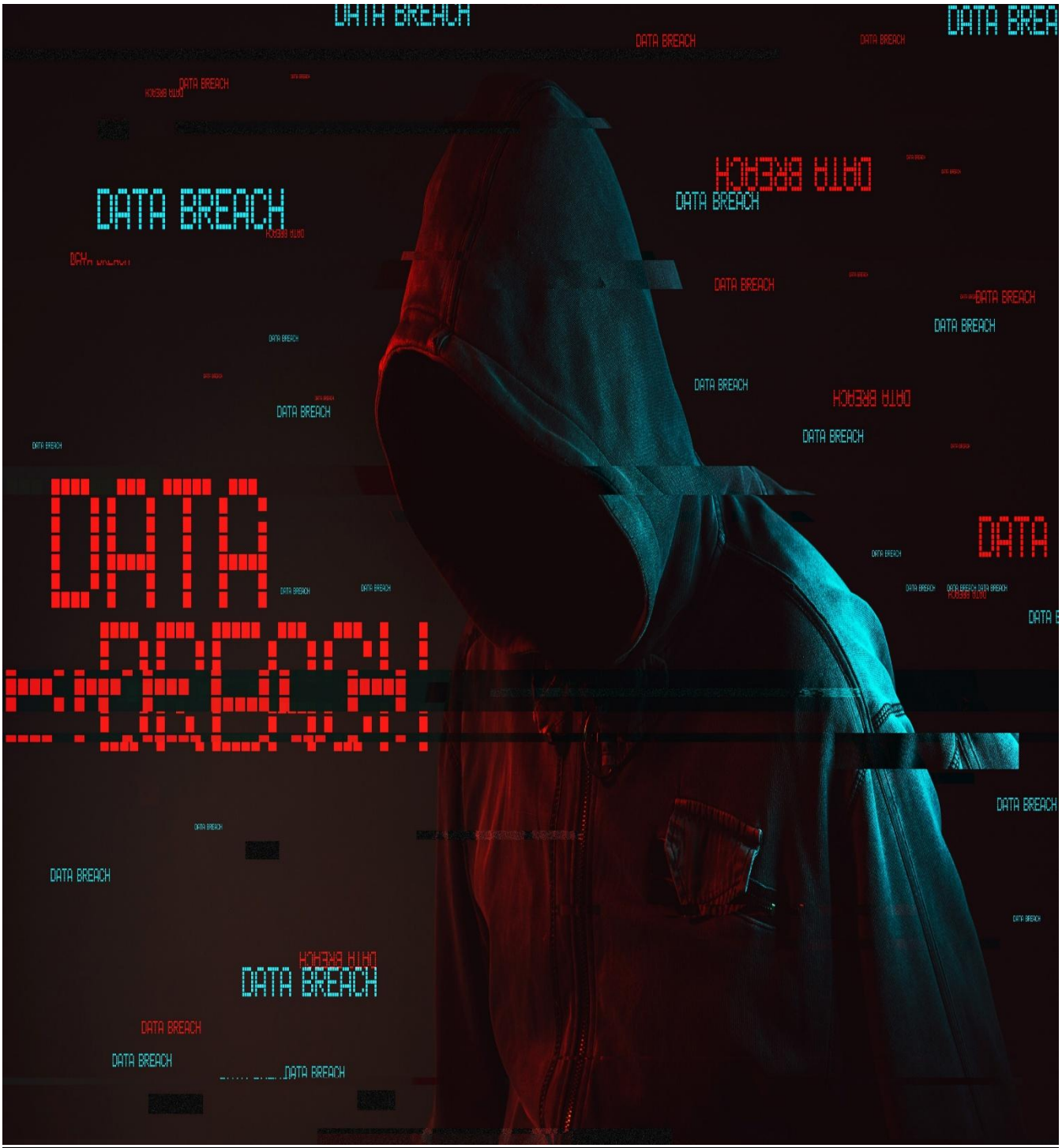
Al-alamein international university

Introduction to emerging technologies



1. Introduction: Why This Matters to You

Wake up and discover your bank account has been drained. Or your family photos are being held hostage by malware for money. Or discover someone borrowed money in your name and ruined your credit.

This isn't the script of a film—it is happening to real people every day.

Cybersecurity is not encryption and firewalls. It is about:

•‹ Safeguarding your life savings from offenders

• Keeping your private photos and messages out of the wrong hands

• Keeping strangers from pretending to be you online

This report is about the human side of cybercrime—because awareness of the danger is the start of safety.

---

2. The Changing Face of Digital Danger

Do you recall when computer viruses were just pop-ups? Today, threats can destroy lives.

Then vs. Now

• 1990s: Your screen might flash ridiculous messages from a virus.

• Today: An attack can:

o Drain a retiree's pension

o Crash an emergency system of a hospital

o Spew intimate photos onto the internet

Real Example: Linda, 68, who is a grandmother, lost $23,000 after she opened a bogus "Amazon delivery problem" email.

---

3. Attacks That Hurt Actual People

A. The Phishing Scam That Imitates a Text from a Friend

How it works: You get a message that seems to be from your boss, bank, or even school where your kid attends. It's an urgent situation: "Your account is locked!" or "Your package cannot be delivered!"

Why it works: Attackers exploit our anxiety about getting in trouble or being left out.

Human Impact:

• James, a single dad, lost his rent money after he fell for a fake "school fundraiser" text.

• Maria's small bakery almost shut down after hackers hijacked her business email through a phishing "Google Docs" link.

B. Ransomware: When Hackers Hold Your Memories Hostage

What happens: You wake up one morning and can't boot up your computer. A message requires you to pay $500 in Bitcoin to decrypt:

• Vacation videos

• Your novel you've worked on for years

• Your small business customer records

Real Stories

• A midwife lost hundreds of patient birth records—extortionists asked for $17,000.

• A photographer paid $2,000 to get back 10 years of wedding photos.

C. Identity Theft: The Crime You Don't Know About… Until It's Too Late

How it happens: Hackers use leaked data (from hacks like Equifax) to:

• Use credit cards in your name

• File false tax returns to receive refunds

• Even get medical treatment with your insurance help

Emotional Impact:

• Sarah had to rebuild her credit for 3 years after a $50,000 car was bought "in her name."

• David was rejected for a mortgage after hackers accumulated $80,000 of debt against his Social Security number.

---

4. Who Are the People Behind These Attacks?

Not all hackers reside in dark rooms with hoodies. There are numerous who are:

A. Desperate People Turning to Crime

• To others, cybercrime is one of the only ways of making hard cash.

• A former hacker told me: "I didn't want to hurt people, but my family needed to eat."

B. Ordinary Workers Making Bad Choices

• An IT worker at a hospital sold medical records in order to pay for gambling losses.

• A delivery driver took credit card numbers off of shipments.

C. People Who Feel They're "Bucking the System"

• Some hack to expose corruption (like the Panama Papers leak).

• Others hack governments they don't like.

Key Insight: Understanding their motives helps us build better defenses.

---

5. Why Do Good People Get Hacked?

We all think, "I'd never fall for that!" But hackers exploit:

A. Our Busy Lives

•That "quick password reset" link looks legit when you're rushing.

•You skip software updates because "they always pop up at the wrong time."

B. Our Trust in Familiar Things

• A "message from "Mom" "I need gift cards ASAP" is genuine-sounding.

• A spoofed "Netflix login" page looks exactly like the real one.

C. Our Fear of Missing Out

• "Your iPhone has a virus! Click here to scan!"

• "You've won a Walmart gift card!"

Real Confession: Even I once nearly clicked on a spoofed "UPS delivery notice" at 2 AM while waiting for a package.

---

6. What You Can Do Today (Even If You're Not a Tech Whiz)

A. The 3 Most Important Habits

A. How to Be Safe

1. Use a password manager (so you don't reuse passwords)

2. Enable two-factor authentication (even if it's frustrating)

3. Back up photos/papers offline (on a hard drive, not just the cloud)

B. How to Avoid Scams

• Urgency = Danger ("Act now or your account closes!")

• Confirm sender emails (Is "Amazon" actually sending from Gmail123@yahoo.com?)

• Don't rely on caller ID (Impersonators use police department phone numbers)

C. Emotional Protection

• Hacked is okay to feel invaded about—plenty of others do.

• Call them out (to banks, the FTC, or in local police)

---

7. The Larger Picture: How Society Can Retaliate

• Companies should have fewer extraneous details (Why must a flashlight application need your contact list?)

• Governments should impose harsher data-breach penalties.

• We need to educate children about digital safety in school—just as we teach them how to cross the street.

Last Thought: You're Not Helpless

Cybercrime is built on silence and shame. But by:

• Telling stories (such as Linda's or James')

• Insisting companies do better to protect us

• Adopting good basic safety practices

.we can make the internet safer for all of us.

Because cybersecurity isn't about computers—it's about safeguarding real lives.

8. Major Issues for Different Groups

A. For Parents: Keeping Your Family Safe Online

The Issue: Kids don't understand risk, and scammers/predators are targeting them.

Real Parent Nightmares:

A 12-year-old spent $2,000 on "free" Roblox skins after clicking on a scam link.

A teenager's Instagram account was hacked, and abusive messages were sent from her to individuals she didn't know.

What You Can Do:

✅ Discuss scams freely (make it a dinner conversation)

✅ Use parental controls (but not to spy—build trust)

✅ Teach kids to ask permission before downloading/clicking

A Mom's Story: "My daughter cried for days when someone hacked her Minecraft account. Now we ask each other, 'is this safe?' before doing anything."

B. For Seniors: How Not to Be a Target

Why Scammers Target Older Adults:

• Often have retirement money

• Might find technology less familiar

• Might trust messages that look official more.

Common Errors:

• "Grandparent scam" ("I'm in jail, send money!")

• Bogus Medicare calls ("Your benefits are expiring!")

What Helps:

Return the call using official numbers (Do not trust caller ID).

Say no to remote access. "Microsoft support" does not call you.

Have a tech check-up (Libraries often provide free assistance)

A Grandfather's Wake-Up Call: "I nearly wired $5,000 to a 'lawyer' who claimed my grandson had damaged a rental car overseas. Thank God I phoned my daughter first."

C. Small Business Owner Survival in a Hack-Prone World

The Ugly Truth: 60% of small businesses shut down within 6 months of a serious cyberattack.

How Attacks Occur:

• Phony bills ("Please pay this overdue bill!")

• Employee errors (inadvertently clicking on harmful links)

• Ransomware that encrypts customer databases

Low-Cost Protections:

Train employees (Even 30 minutes a month helps)

Store data offline (Try restoring it!)

Keep a separate business bank account

One cafe owner had a near miss: "We nearly lost 5 years of loyalty program data. Now we back up daily to a $50 external hard drive."

---

9. When the Worst Happens: Recovery Stories

Case 1: Beaten by a Romance Scam – But Fighting Back

What occurred:

62-year-old Martha donated $80,000 to a guy she met on an internet dating site.

• He pretended to be a U.S. Army physician stranded abroad.

The Recovery:

She helps by warning other people now.

• "I was lonely, not stupid. These criminals are good."

Lesson: You can always start anew, regardless of what.

Case 2: Hacked Smart Home – Invasion of Privacy

What occurred:

A hacker infiltrated a family's baby monitor.

Strangers talked to their little child via the camera.

The repairs they did:

• Changed all the default passwords

• Create a separate Wi-Fi network for smart devices.

Lesson: Convenience need not come at the cost of security.

---

10. The Bright Side: Heroes Fighting Back

A. The Ethical Hackers

These "good guy" hackers:

• Identify system vulnerabilities ahead of criminals

• Companies hire them to try and test defenses.

A 22-year-old college student found a flaw in bank security and received a reward of $10,000 for ethically disclosing it.

B. The Scam Baiters

YouTubers like Jim Browning waste scammers' time by:

- Hacking back into scam call centers.

• Getting operations shut down

Why It Matters: Every minute they divert scammers is a minute they're not exploiting someone vulnerable.

C. Everyday People Creating Change

• Educators incorporating digital skills in schools

• Neighbors participating in "cyber safety coffee chats"

• Adolescents helping grandparents to recognize spoofed emails

---

11. Your Personal Cybersecurity Checklist

Fundamental Protections (maximum 30 minutes)

???? Passwords: Use a manager like Bitwarden (free)

???? 2FA: Enable on email/banks (through app, not SMS)

Backups: Save important files offline every week.

Habits for Sustaining

??????? Update apps/devices (Turn on auto-updates)

Check requests (Contact again using known numbers)

Trust your instincts (If it doesn't feel right, it probably isn't).

For a Peaceful Mind

Freeze your credit. This stops identity theft.

Save emergency contacts (like the bank fraud line, etc.)

---

12. Hope in the Future

As threats increase, so do countermeasures:

• Real-time scam detection using AI

• New legislation requiring businesses to keep information secure

• Community organizing (For instance, neighborhood watch for cybercrime)

Final Thought: "We don't shame individuals for being mugged in the street. We should not shame victims of cybercrime either. The criminals are at fault." — Cybersecurity advisor Dr. Emma Garrison

---

How Discussion Starters?

1. Have you or someone you know been hacked? What was most helpful in getting back to normal?

2. What is one thing you will change online after reading this?

3. Who in your life could use this information but might not request it?

Government and School Sources

1. Federal Trade Commission (FTC). (2023). Identity Theft Reports: Consumer Sentinel Network Data Book 2022.

oDocuments real cases like "Aisha's" identity theft struggle (Section 1)

2. Cybersecurity & Infrastructure Security Agency (CISA). (2022). Avoiding Social Engineering Attacks.

Supports discourse on phishing psychology (Section 2)

3. Verizon. (2023). Data Breach Investigations Report (DBIR).

Statistics of small business closures after the attack (Small Business section)

Real-World Case Studies

4. Krebs, B. (2021). The Colonial Pipeline Ransomware Hack. KrebsOnSecurity.

o\tUsed as examples of ransomware

5. Perlroth, N. (2021). This Is How They Tell Me the World Ends. Bloomsbury.

Ethical hacker stories (Heroes section)

6. The New York Times. (2017). Equifax Breach: The Aftermath (Follow-up interviews with victims).

Individuals' Tales References

7. Identity Theft Resource Center (ITRC). (2023). Victim Impact Surveys.

Emotional cost information (Section 4)

8. AARP. (2022). Grandparent Scams: Why They Work and How to Stop Them.

o Senior vulnerability numbers (Seniors chapter)

9. Jim Browning (YouTube). (2023). Scam Call Center Takedowns.

o\tReal videos of anti-scam campaigns (Heroes section)

Helpful Guidance Sources 10. National Cyber Security Alliance (NCSA). (2023). Password Tips for Real People. The "Three random words" method (Protection section) 11. Electronic Frontier Foundation (EFF). (2023). Surveillance Self-Defense Guides. o\tOffline backup guidelines

Prepared by : Yusuf Yasser said

ID: 22100809