INSIDE A HACKER'S MIND

Understanding how cybercriminals target you

Educational Community
ALLIANCE CREDIT UNION

EDUCACU.COM | 419-381-2323
3845 Angola Road, Toledo, OH 43615

THIS MONTH'S TOPICS:

Cybercriminals are always one step ahead, using deception and sophisticated tactics to break into systems and steal data. But what if you could think like a hacker and recognize their methods before they strike?

Malicious actors don't just rely on brute force to break into systems. They exploit human psychology, technical weaknesses, and everyday habits that many people overlook. A single careless click or an over-shared piece of personal information can open the door to harm. Understanding how these criminals operate is essential to staying ahead of their schemes.

Ethical hacking is used to detect and mitigate security vulnerabilities before they can be exploited by malicious actors. Ethical hackers, whether working within organizations or as external consultants, leverage their expertise to evaluate the security of systems, networks, and applications, offering insights and recommendations to strengthen cybersecurity. Check out the diagram below to learn how ethical hacking works.

5 PHASES OF ETHICAL HACKING

1
Reconnaissance
The hacker gathers information and data about a target before launching an attack

2
Scanning
The hacker identifies a quick way to gain access to the network and look for information

3
Gaining Access
The hacker launches an assault on the system or network and gains access to the system

4
Maintaining Access
The hacker maintains access to the system until the hacker's objective is achieved

5
Covering Tracks
The hacker removes all signs of harmful behavior in order to avoid detection

Ethical hacking gives us a glimpse into a malicious hacker's process. Understanding the steps taken not only enhances threat detection and response, but also fosters a culture of continuous improvement in cybersecurity strategies. In an era where cyber threats are constantly evolving, ethical hacking serves as a vital tool for staying ahead of attackers and safeguarding sensitive data and critical systems. Think like a hacker (an ethical one), and make sure your systems are protected.

Social Media
OVERSHARING

Oversharing on social media can lead to identity theft, social engineering, spear phishing, and more. Below are some examples of oversharing that could compromise your cyber safety.

- Posting your geographic location and trip details when traveling.
- Posting work-related information on your personal account.
- Posting your interests, hobbies, activities, and where those activities take place.
- Posting intimate details about yourself, including your thoughts and secrets.
- Posting about your family members, friendships, relationships, and pets.
- Posting pictures of your vehicle, especially if the license plate is visible.
- Posting pictures of your home, especially if your address is visible.

In order to keep yourself safe, make your social media accounts private, curate your “friends” list, monitor new followers, and be thoughtful about what you share. Stay safe out there!

SCAM OF THE MONTH: TOAD ATTACKS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Dr. Karen Patel, an administrator at Westview Medical Group, received an urgent voicemail from a representative claiming to be from MedEquip Solutions, a trusted vendor. The caller warned of an overdue invoice that needed immediate payment to avoid supply delays. Shortly after, Dr. Patel received a follow-up email from billing@medequip-solutions.com, which looked legitimate and included an invoice/payment link. Wanting to prevent disruptions, she called the number from the voicemail, spoke to a representative, and processed the payment via ACH transfer (an electronic transaction that moves funds between banks or credit unions through the Automated Clearing House (ACH) network).

Days later, MedEquip Solutions contacted her about a real outstanding invoice, revealing the previous one was fraudulent. The attackers had used voicemail, email spoofing, and urgency tactics to manipulate Dr. Patel into wiring $18,750 to a fake account. This TOAD attack succeeded by exploiting trust, pressuring quick action, and using caller ID spoofing to appear legitimate.

DID YOU SPOT THE RED FLAGS?

- The caller and email both emphasized immediate payment to avoid supply disruptions.
- The invoice requested an ACH transfer, which is harder to reverse than credit card payments.

STAY SAFE

HOW TO PROTECT YOURSELF

- Always verify financial requests by contacting the vendor or sender using a trusted phone number or email, not the one provided to you.
- Be cautious of urgent financial requests, especially from new or altered communication channels.

SIGNS YOU'VE BEEN HACKED!

1. Slow System Performance
2. Ransomware Messages
3. Strange Account Behavior
4. Unfamiliar Software Installations
5. Your Browser Home Page is Different
6. Missing Files

Recognizing signs of a security breach is crucial, but acting quickly is just as important. If you notice slow system performance, strange pop-ups, or unfamiliar programs installed on your device, don't ignore them. These could be signs of malware running in the background, siphoning data or consuming resources. Sudden changes to your browser home page or missing files may indicate unauthorized access, where hackers manipulate your system to redirect you to malicious sites or erase critical data. Unusual account behavior, such as unexpected password reset emails, failed login attempts, or messages sent from your accounts that you didn't write, could signal that a cybercriminal has gained control. In the most alarming cases, ransomware messages demanding payment to unlock your files confirm that your system has been compromised.

If you suspect you've been hacked, disconnect from the internet, run a full security scan, change your passwords, and monitor your accounts for suspicious activity. The sooner you act, the better your chances of minimizing damage and regaining control.